Marco Fontana · Sophie Frisch
Sarah Glaz · Francesca Tartarone
Paolo Zanardo *Editors*

Rings, Polynomials, and Modules

Springer

Rings, Polynomials, and Modules

Marco Fontana • Sophie Frisch • Sarah Glaz
Francesca Tartarone • Paolo Zanardo
Editors

Rings, Polynomials, and Modules

Springer

Editors
Marco Fontana
Dipartimento di Matematica e Fisica
Università degli Studi Roma Tre
Rome, Italy

Sophie Frisch
Department of Analysis and Number Theory
Graz University of Technology
Graz, Austria

Sarah Glaz
Department of Mathematics
University of Connecticut
Storrs, CT, USA

Francesca Tartarone
Dipartimento di Matematica e Fisica
Università degli Studi Roma Tre
Rome, Italy

Paolo Zanardo
Dipartimento di Matematica
Università di Padova
Padova, Italy

ISBN 978-3-319-65872-8 ISBN 978-3-319-65874-2 (eBook)
https://doi.org/10.1007/978-3-319-65874-2

Library of Congress Control Number: 2017957649

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume is the outcome of two conferences: “Recent Advances in Commutative Ring and Module Theory” held in Bressanone/Brixen, Italy, June 13–17, 2016; and “Conference on Rings and Polynomials” held in Graz, Austria, July 3–8, 2016. The volume contains contributed as well as invited papers by the speakers at these conferences, and a small collection of invited papers by some of the leading experts in the area, carefully selected for the impact of their research on the major themes of the conferences.

The aim of the meetings was to present recent progress and new trends in the area of commutative algebra, with emphasis on commutative ring theory, module theory, and integer-valued polynomials along with connections to algebraic number theory, algebraic geometry, topology, and homological algebra. The wide range of topics is reflected in the table of contents of this volume.

The two conferences brought together over one hundred mathematicians from over 20 countries—renowned researchers as well as promising young newcomers—in a pleasant and peaceful atmosphere that engendered many fruitful collaborations.

In addition to the conference participants and authors of papers, a number of other people helped make these conferences and this volume of proceedings possible. Among those we count the organizing and scientific committees of both conferences. The organizing committee of the Bressanone conference consisted of Florida Girolami, Francesca Tartarone, and Paolo Zanardo, while the scientific committee included Valentina Barucci, Dikran Dikranjan, Brendan Goldsmith, Evan Houston, Bruce Olberding, Francesca Tartarone, and Paolo Zanardo. The organizing committee of the Graz conference consisted of Sophie Frisch, Carmelo Finocchiaro, and Roswitha Rissner, while the scientific committee included Karin Baur, Jean-Luc Chabert, Marco Fontana, Alfred Geroldinger, Sarah Glaz, and Irena Swanson. We wish to thank them all for their efforts, without which these conferences would not have taken place and this volume would not have seen the light of day. In addition, the Graz conference editors wish to thank the departmental secretary

Hermine Panzenböck for administrative support and many students for technical support. The Bressanone conference editors wish to extend special thanks to Marco Fontana, Stefania Gabelli, and Luigi Salce for useful suggestion.

We also thank the many organizations who sponsored these conferences and, most importantly, made it possible to provide support for graduate students and mathematicians not supported by their institutions. The Bressanone conference was sponsored by Istituto Nazionale di Alta Matematica (INdAM), the departments of mathematics of Università degli Studi di Padova and Sapienza Università di Roma, and the department of mathematics and physics of Università degli Studi Roma Tre. The Graz conference was sponsored by the Austrian Science Fund (FWF), the Austrian Mathematical Society, the province of Styria, and the faculty of mathematics and physics of Technische Universität Graz.

Last, but not least, we thank the editorial staff of Springer, in particular Elizabeth Loew, for their cooperation, hard work, and assistance with this volume.

Rome, Italy Marco Fontana
Graz, Austria Sophie Frisch
Storrs, CT, USA Sarah Glaz
Rome, Italy Francesca Tartarone
Padova, Italy Paolo Zanardo
July 2017

Contents

Reducing Fractions to Lowest Terms

Daniel D. Anderson and Erik Hasse

Abstract The purpose of this paper is to investigate putting or reducing a fraction to lowest terms in a general integral domain. We investigate the integral domains in which every fraction can be (uniquely) put in or reduced to lowest terms.

Keywords ACCP • Atomic domain • GCD domain • Lowest terms • gcd • Weak gcd

Subject Classifications Primary 13G05, Secondary 13A05, 13F15

We are all familiar with reducing fractions to lowest terms over the integers or polynomials over a field. The purpose of this paper is to study this in the context of general integral domains. We investigate when a fraction a/b can be put in lowest terms c/d (i.e., $a/b = c/d$ where c and d are relatively prime) or reduced to lowest terms $(\frac{a}{d})/(\frac{b}{d})$ (i.e., $(\frac{a}{d})/(\frac{b}{d})$ is in lowest terms for some common divisor d of a and b) and when the lowest terms representation for a/b is "unique". Of particular interest are the integral domains in which every fraction can be reduced to lowest terms.

Throughout D will be an integral domain with quotient field K. Let $a, b \in D^* := D - \{0\}$. We denote the gcd of a and b by $[a, b]$, if it exists. Of course, $[a, b]$ is only unique up to a unit factor. We write $[a, b] = 1$ ($[a, b] \neq 1$) if a and b are (not) relatively prime. A common divisor d of a and b is a *weak gcd for a and b* if $\left[\frac{a}{d}, \frac{b}{d}\right] = 1$. And D is a (*weak*) *GCD domain* if every pair $a, b \in D^*$ has a (weak) gcd. For a nonzero fractional ideal I of D, $I^{-1} := \{x \in K | xI \subseteq D\}$ and $I_v := (I^{-1})^{-1} = \cap\{Dx | x \in K \text{ with } I \subseteq Dx\}$. If $(a, b)_v = (d)$ (or equivalently $\text{lcm}(a, b) = \frac{ab}{d}$), then $[a, b] = d$, but not necessarily conversely (see Example 2). However, if D is a GCD domain with $[a, b] = d$, then $(a, b)_v = (d)$. We remark that the following three conditions are equivalent: (1) $\text{lcm}(a, b)$ exists, (2) $(a) \cap (b)$ is principal, and (3) $(a, b)_v$ is principal. And in this case $((a) \cap (b))\,(a, b)_v = (a)(b)$.

D.D. Anderson (✉) • E. Hasse
Department of Mathematics, The University of Iowa, Iowa City, IA, USA
e-mail: dan-anderson@uiowa.edu; erik-hasse@uiowa.edu

M. Fontana et al. (eds.), *Rings, Polynomials, and Modules*,
https://doi.org/10.1007/978-3-319-65874-2_1

If $(a, b) = (d)$, then $(a, b)_v = (d)$, but not conversely. A nonzero nonunit a of D is *irreducible* or an *atom* if $a = bc$ implies b or c is a unit and D is *atomic* if each nonzero nonunit of D is a finite product of atoms. An integral domain D satisfies the *ascending chain condition on principal ideals* (*ACCP*) if every ascending chain $(a_1) \subseteq (a_2) \subseteq \cdots$ of principal ideals of D stabilizes. And D is a *Bezout domain* if every finitely generated ideal, equivalently, every two-generated ideal of D, is principal. Thus a Bezout domain is a GCD domain in which the gcd for each pair a, b is a linear combination of a and b.

We begin with the following definitions.

Definition 1 Let D be an integral domain and let $a, b, c, d, e, f \in D^*$. We say that *a/b can be put in the form c/d* if $a/b = c/d$ and that *a/b can be reduced to the form c/d* if there is a common divisor e of a and b with $c = \frac{a}{e}$ and $d = \frac{b}{e}$. The fraction a/b is in (*strong, resp., absolute*) *lowest terms* if $[a, b] = 1$ ($(a, b)_v = D$, resp., $(a, b) = D$). Thus a/b can be put in lowest terms if $a/b = c/d$ where $[c, d] = 1$ and a/b can be reduced to lowest terms if $a/b = c/d$ where $c = \frac{a}{e}$ and $d = \frac{b}{e}$ for some common divisor e of a and b and $[c, d] = 1$. We will then sometimes say that c/d is a (reduced) lowest terms for a/b. Similar statements hold for strong and absolute lowest terms. The fraction a/b has *essentially unique* (*strong, resp., absolute, reduced*) *lowest terms* if there exists at least one c/d in (strong, resp., absolute, reduced) lowest terms with $a/b = c/d$ and if $a/b = e/f$ where e/f is in (strong, resp., absolute, reduced) lowest terms, then $e = uc$ and $f = ud$ for some unit u of D.

Remark 1 Let $a, b \in D$ with b nonzero. There is some ambiguity in the notation a/b as to whether a/b just denotes an element of K or the particular representation of that element. Indeed, an element $x \in K$ has many representations in the form a/b with $a/b = c/d \Leftrightarrow ad = bc$ ($a, b, c, d \in D$, b, d nonzero). However, when we write a/b we will usually mean the particular representation, even though we write $a/b = c/d$ to mean they are equal as an element of K, i.e., $ad = bc$.

Definition 2 The integral domain D is a *lowest terms* (*LT*) *domain* (resp., *reduced lowest terms* (*RLT*) *domain*) if each nonzero fraction a/b ($a, b \in D^*$) can be put in (resp., reduced to) lowest terms. And D is a *unique lowest terms* (*ULT*) *domain* if each nonzero fraction a/b ($a, b \in D^*$) has essentially unique lowest terms.

Remark 2 In an obvious way we could have defined the following integral domains: unique reduced lowest terms domain, strong (resp., absolute) lowest terms domain, unique strong (resp., absolute) lowest terms domain, reduced strong (resp., absolute) lowest terms domain, and unique reduced strong (resp., absolute) lowest terms domain. The reason we have not is because by Theorem 1 (5, resp., 6) they (resp., the last four) are all equivalent to the integral domain being a GCD domain (resp., Bezout).

Remark 3 So far we have only considered nonzero fractions a/b ($a, b \in D^*$). Suppose that $a = 0$ and consider $0/b$ where $b \in D^*$. Since $[0, b] = b$, $(0, b)_v = (b)$ and $(0, b) = (b)$, we see (with the obvious extension of the definitions in Definition 1) that $0/b$ can be reduced to $0/1$ and $0/b$ has essentially unique (strong resp., absolute) lowest terms $0/1$. Thus there is no loss in generality in only considering nonzero fractions.

We next determine when a fraction can be put in or reduced to (strong, absolute) lowest terms.

Theorem 1 *Let D be an integral domain and let $a, b, c, d, e, f \in D^*$.*

1. *a/b can be put in lowest terms if and only if there exists an $s \in D^*$ so that sa and sb have a weak gcd. If d is a weak gcd for sa and sb, then $a/b = \left(\frac{sa}{d}\right) / \left(\frac{sb}{d}\right)$ and the last fraction is in lowest terms. So D is an LT domain if and only if for each $a, b \in D^*$, there exists $s \in D^*$ so that sa and sb have a weak gcd.*
2. *a/b can be reduced to lowest terms if and only if a and b have a weak gcd. If a and b have a weak gcd d, then $a/b = \left(\frac{a}{d}\right) / \left(\frac{b}{d}\right)$ and the last fraction is in lowest terms. So D is an RLT domain if and only if D is a weak GCD domain.*
3. *The following are equivalent:*

   a. *$[a, b]$ exists, and*
   b. i. *If c is a common divisor of a and b, then $\left(\frac{a}{c}\right) / \left(\frac{b}{c}\right)$ can be reduced to lowest terms and*
      ii. *a/b has essentially unique reduced lowest terms.*

4. *a/b is in strong lowest terms if and only if $a/b = c/d$ implies there exists $e \in D^*$ with $c = ea$ and $d = eb$.*
5. a. *The following are equivalent:*

      i. *$(a, b)_v$ is principal (or equivalently, $(a) \cap (b)$ is principal or $\operatorname{lcm}(a, b)$ exists),*
      ii. *a/b can be reduced to strong lowest terms, and*
      iii. *a/b can be put in strong lowest terms.*

      If $(a, b)_v = (d)$, then $a/b = \left(\frac{a}{d}\right) / \left(\frac{b}{d}\right)$ where the last fraction is in strong lowest terms. Moreover, this strong lowest terms representation is unique in the following sense. If $a/b = e/f$ where $[e,f] = 1$, then $e = u\left(\frac{a}{d}\right)$ and $f = u\left(\frac{b}{d}\right)$ where u is a unit of D. Hence e/f is actually a strong lowest terms representation for a/b.

   b. *For the integral domain D, the following are equivalent:*

      i. *G is a GCD domain,*
      ii. *Every nonzero fraction of D can be reduced to strong lowest terms,*
      iii. *Every nonzero fraction of D can be put in strong lowest terms,*
      iv. *Every nonzero fraction of D has a essentially unique reduced lowest terms.*
      v. *D is an RLT domain and a ULT domain.*

6. a. *The following are equivalent:*

      i. *(a, b) is principal,*
      ii. *a/b can be reduced to absolute lowest terms, and*
      iii. *a/b can be put in absolute lowest terms.*

If $(a, b) = (d)$, then $a/b = (\frac{a}{d})/(\frac{b}{d})$ where the last fraction is in absolute lowest terms. Moreover, this absolute lowest terms representation is unique in the following sense. If $a/b = e/f$ where $[e,f] = 1$, then $e = u(\frac{a}{d})$ and $f = u(\frac{b}{d})$ where u is a unit of D. Hence e/f is actually an absolute lowest terms representation for a/b.

b. *For an integral domain D, the following are equivalent:*

   i. *D is a Bezout domain,*
   ii. *Every nonzero fraction of D can be reduced to absolute lowest terms,*
   iii. *Every nonzero fraction of D can be put in absolute lowest terms.*

Proof (1) Suppose there exists an $s \in D^*$ with sa and sb having weak gcd d. Then $\left[\frac{sa}{d}, \frac{sb}{d}\right] = 1$ and $a/b = sa/sb = \left(\frac{sa}{d}\right) / \left(\frac{sb}{d}\right)$. So a/b can be put in lowest terms. Conversely, suppose that a/b can be put in lowest terms c/d. Now $a/b = c/d$ implies $ad = bc$ and so $a|bc$. Thus a is a common divisor of ac and bc and $\left[\frac{ac}{a}, \frac{bc}{a}\right] = [c, d] = 1$, i.e., a is weak gcd of ac and bc. The last statement is now immediate.

(2) Note that d is a weak gcd for a and b if and only if d is a common divisor of a and b with $\left[\frac{a}{d}, \frac{b}{d}\right] = 1$. This just says that $a/b = \left(\frac{a}{d}\right) / \left(\frac{b}{d}\right)$ where the last fraction is in lowest terms. This proves the first statement and the second statement is now immediate.

(3) $(a) \Rightarrow (b)$ If $[a, b]$ exists and c is a common divisor of a and b, then $\left[\frac{a}{c}, \frac{b}{c}\right]$ exists and hence is the unique weak gcd for $\frac{a}{c}$ and $\frac{b}{c}$. Then apply (2).

$(b) \Rightarrow (a)$ Let $a, b \in D^*$. Since a/b can be reduced to lowest terms, by (2), a and b have a weak gcd d. We show that $[a, b] = d$. Certainly d is a common divisor of a and b. Suppose e is a common divisor of a and b. Then $\left(\frac{a}{e}\right) / \left(\frac{b}{e}\right)$ can be reduced to lowest terms, so again by (2) there is an $f \in D^*$ with $\left[\frac{a}{ef}, \frac{b}{ef}\right] = 1$. Now $\left(\frac{a}{d}\right) / \left(\frac{b}{d}\right) = a/b = \left(\frac{a}{ef}\right) / \left(\frac{b}{ef}\right)$ where the first and third fractions are in lowest terms. By uniqueness $\frac{a}{d} = u\frac{a}{ef}$ for some unit u. Hence $d = u^{-1}ef$, so $e|d$. Thus $[a, b] = d$. (We have shown that for $a, b \in D^*$, $[a, b]$ exists if and only if a and b have a unique (up to associates) weak gcd and for every $c|a, b$, $\frac{a}{c}$ and $\frac{b}{c}$ have a weak gcd.)

(4) $(\Rightarrow) a/b = c/d$ implies $ad = bc$, so $a|bc$. Since $(a, b)_v = D$, $a|c$ (see Remark 4). So $c = ea$ for some $e \in D^*$ and hence $d = \frac{bc}{a} = eb$. $(\Leftarrow)$ Suppose that $(a, b) \subseteq (\alpha/\beta)$ for $\alpha, \beta \in D^*$. Then $\beta(a, b) \subseteq (\alpha)$, so $a\beta = c\alpha$ and $b\beta = d\alpha$ for some $c, d \in D^*$. So $a/b = a\beta/b\beta = c\alpha/d\alpha = c/d$. Hence $c = ax$, and $d = bx$ for some $x \in D^*$. Then $a\beta = ax\alpha \Rightarrow \beta = x\alpha \Rightarrow \alpha/\beta = 1/x$. So $D \subseteq (\alpha/\beta)$. Hence $(a, b)_v = D$.

(5) (a) (i)$\Rightarrow$(ii) Suppose $(a, b)_v = (d)$. Then $d|a$ and $d|b$ and $\left(\frac{a}{d}, \frac{b}{d}\right)_v = \frac{1}{d}(d) = D$; so $a/b = \left(\frac{a}{d}\right) / \left(\frac{b}{d}\right)$ where the last fraction is in strong lowest terms. (ii)$\Rightarrow$(iii) Clear. (iii)$\Rightarrow$(i) Suppose $a/b = c/d$ where $(c, d)_v = D$. Now $ad = bc$ and $(c, d)_v = D$ implies $(a) = (ac, ad)_v = (ac, bc)_v = (a, b)_v c$; so $(a, b)_v = \left(\frac{a}{c}\right)$ is principal. This proves the equivalence of (i)–(iii) and the second statement. Next suppose $(a, b)_v = (d)$ and $a/b = e/f$ where $[e,f] = 1$. Now $e/f = a/b = \left(\frac{a}{d}\right) / \left(\frac{b}{d}\right)$

where $[e,f] = 1$ and $\left(\frac{a}{d}, \frac{b}{d}\right)_v = D$. By (4) $e = \frac{a}{d}g$ and $f = \frac{b}{d}g$ for some $g \in D^*$ So $1 = [e,f] = \left[\frac{a}{d}g, \frac{b}{d}g\right]$. Hence g must be a unit.

(b) The equivalence of (i)–(iii) and (i)⇒(iv),(v) follow from (a). (iv),(v)⇒(i) follows from (3).

(6) (a) This is similar to the proof of 5(a). Indeed, we can just delete the "subscript" v wherever it occurs.

(b) This follows from 6(a).

Remark 4 The proof of Theorem 1 (4) used the well-known fact that for $a, b, c \in D^*$ with $(a, b)_v = D$, then $a|bc \Rightarrow a|c$. For suppose $ar = bc$ for some $r \in D^*$. Then $(c) = c(a, b)_v = (ac, bc)_v = (ac, ar)_v \subseteq (a)$; so $a|c$. It is interesting to note that the converse is also true: If $a|bc \Rightarrow a|c$ for all $c \in D^*$, then $(a, b)_v = D$. As we will not need this result, the proof is left to the reader.

Thus it is not true in general that $a|bc$ with $[a, b] = 1$ implies $b|c$. The "proof" breaks down because $[a, b] = 1$ does not imply that $[ac, bc] = c$. If fact, for $a, b \in D^*$, $[ac, bc]$ exists for all $c \in D^*$ if and only if $(a, b)_v$ exists [1, Theorem 2.1]. It is easy to check that if $[ac, bc]$ exists, then $[a, b]$ exists and $[ac, bc] = [a, b]c$. If d is a (weak) gcd for a and b and $c|d$, then $\frac{d}{c}$ is a (weak) gcd for $\frac{a}{c}$ and $\frac{b}{c}$.

The above paragraphs explain why a/b having a strong lowest terms representation forces $(a, b)_v$ to be principal while a/b having a lowest terms representation does not force $[a, b]$ to exist.

Remark 5 An integral domain R is said to satisfy *Property D* if whenever $a, b, c \in R^*$ with $[a, b] = 1$ and $a|bc$, then $a|c$. Property D is equivalent to a number of other properties slightly weaker than being a GCD domain such as PSP2*:* $a, b \in R^*$ with $[a, b] = 1$ implies $(a, b)_v = R$ (also called Property λ in [5]). Property D implies that atoms are prime, so an atomic domain satisfying Property D is a UFD, and conversely. See [2] for a thorough investigation of these related properties. Via Theorem 1 (3)(a) the following are equivalent: (1) R satisfies PSP2, (2) if a fraction a/b ($a, b \in R^*$) can be put in lowest terms, it can be put in strong lowest terms, and (3) any lowest terms representation of a fraction a/b ($a, b \in R^*$) is actually a strong lowest terms representation.

Remark 6 R. Gilmer briefly considers fractions in (strong) lowest terms in [4, Exercise 5, p.183]. Let D be an integral domain and $a, b \in D^*$. There he defines a fraction a/b to be *irreducible* if $[a, b] = 1$ and to be in *canonical form* if $a/b = c/d$ for $c, d \in D^*$ implies there is a $x \in D^*$ with $c = ax$ and $d = bx$. The exercise asks to show that a/b is in canonical form if and only if $(a, b)_v = D$ which is our Theorem 1 (4) and that every fraction can be put in canonical form if and only if D is a GCD domain which is $(i) \Leftrightarrow (iii)$ of our Theorem 1 (5)(b).

Remark 7 We can give a star-operation version of Theorem 1 (5,6). Recall that a *star-operation* $\star$ on D is a closure operation $\star$ on the set $F(D)$ of nonzero fractional ideals of D that satisfies $(aA)^\star = aA^\star$ and $(a)^\star = (a)$ for $a \in K^*$ and $A \in F(D)$. Examples of star-operations include the *v-operation* $A \to A_v$ and the *d-operation*

$A \to A_d = A$. For an introduction to star-operations, see [4, Section 32]. For $a, b \in D^*$, we say that a/b is in $\star$-*lowest terms* if $(a, b)^\star = D$. Then a/b can be put in (equivalently, reduced to) $\star$-lowest terms if and only if $(a, b)^\star$ is principal. Thus every fraction a/b can be put in (equivalently, reduced to) $\star$-lowest terms if and only if every nonzero doubly generated (equivalently, finitely generated) ideal A has $A^\star$ principal. Here Theorem 1 (5, resp., 6) is just the case where $\star = v$ (resp., d).

We next show the ubiquity of RLT domains.

Theorem 2 *Let D be an integral domain. If D is a GCD domain or satisfies ACCP, then D is a weak GCD domain and hence is an RLT domain.*

Proof The case where D is a GCD domain is immediate, so assume that D satisfies ACCP. Suppose there exists $a_0, b_0 \in D^*$, so that a_0, b_0 do not have a weak gcd. Then the set $S = \{(a) | a \in D^*,$ there exists a $b \in D^*$ so that a, b do not have a weak gcd$\}$ is a nonempty set of proper principal ideals. Let (a) be a maximal element of S. So there exists a $b \in D^*$ so that a, b do not have a weak gcd. In particular, $[a, b] \neq 1$. So there is a nonunit $e \in D^*$ with $e|a$ and $e|b$. But then $\frac{a}{e} \in D^*$ with $\left(\frac{a}{e}\right) \supsetneq (a)$. So either $\frac{a}{e}$ is a unit or $\left(\frac{a}{e}\right)$ is a proper principal ideal of D. Thus $\frac{a}{e}$ and $\frac{b}{e}$ have a weak gcd d, so $\left[\frac{a}{ed}, \frac{b}{ed}\right] = 1$. So ed is a weak gcd for a and b, a contradiction.

Corollary 1 *An integral domain D is a UFD if and only if D satisfies ACCP and D is a ULT domain.*

Proof ($\Rightarrow$) Suppose D is a UFD. It is well known that D satisfies ACCP and since a UFD is a GCD domain, D is a ULT domain by Theorem 1 (4). ($\Leftarrow$) Since D satisfies ACCP, D is an RLT domain by Theorem 2. So D is an RLT domain and a ULT domain. By Theorem 1 (4), D is a GCD domain. But a GCD domain satisfying ACCP is a UFD.

We next give an example of an integral domain that is not an LT domain. We later use this example to give an example (Example 4) of an integrally closed atomic domain that is not an LT domain.

Example 1 (An Integral Domain That is Not an LT Domain) Let D be the integral domain $k[X, Y, Z][\{\frac{X}{Z^n}, \frac{Y}{Z^n}\}_{n \geq 1}]$ where k is a field and X, Y, Z are indeterminates over k. Then we cannot write $X/Y = a/b$ where $a, b \in D^*$ with $[a, b] = 1$. For suppose $X/Y = a/b$ for $a, b \in D^*$. We can write $a = f/Z^m$ and $b = g/Z^n$ where $f, g \in k[X, Y, Z]^*$ and $m, n \geq 0$. Then $XgZ^m = YfZ^n$. Then $X|f$ and $Y|g$ in $k[X, Y, Z]$ and hence $\frac{X}{Z^m}|a$ and $\frac{Y}{Z^n}|b$ in D. But $Z|\frac{X}{Z^m}$ and $Z|\frac{Y}{Z^n}$ in D, so $Z|a$ and $Z|b$ in D. Hence $[a, b] \neq 1$.

By Corollary 1, any integral domain satisfying ACCP that is not a UFD is an RLT domain that is not a ULT domain. We next examine a concrete example.

Example 2 (An RLT Domain That is Not a ULT Domain) Let $D = k[X^2, X^3]$ where k is a field and X is an indeterminate over k. Then D is Noetherian and hence satisfies ACCP and thus is an RLT domain. Here X^2 and X^3 are irreducible, with $X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$, so R is not a UFD and hence not a ULT domain. Indeed $X^4/X^3 = X^3/X^2$

where $[X^3, X^4] = [X^2, X^3] = 1$. Now $[X^4, X^5] = X^2$, but $[X^5, X^6]$ does not exist. In fact, both X^2 and X^3 are weak gcds for X^5 and X^6 since $\left[\frac{X^5}{X^2}, \frac{X^6}{X^2}\right] = \left[X^3, X^4\right] = 1$ and $\left[\frac{X^5}{X^3}, \frac{X^6}{X^3}\right] = [X^2, X^3] = 1$. Moreover, X^6/X^5 can be reduced to both X^4/X^3 and X^3/X^2, each of which is in lowest terms, but there does not exist a unit $u \in D$ with $X^3 = uX^4$ and $X^2 = uX^3$. Here X^4/X^3 can be put in lowest terms form X^3/X^2, but cannot be reduced to the lowest terms form X^3/X^2. Note that $[X^2, X^3] = 1$, but $(X^2, X^3)_v = (X^2, X^3) \neq D$ and $(X^2) \cap (X^3) = (X^5, X^6)$ is not principal. In fact, by Theorem 1 (5)(a) we cannot write $X^3/X^2 = f/g$ where $f, g \in D^*$ with $(f, g)_v = D$.

We have made a distinction between putting a fraction in lowest terms and reducing a fraction to lowest terms. We now give an example of a fraction that can be put in lowest terms but cannot be reduced to lowest terms.

Example 3 (A Fraction That Can Be Put in, But Not Reduced to, Lowest Terms) Let $D = k[X, Y, Z, T][\frac{X}{T}, \frac{Y}{T}, \{\frac{X}{Z^n}, \frac{Y}{Z^n}\}_{n \geq 1}]$ where k is a field and $X, Y, Z,$ and T are indeterminates over k. Then T is a weak gcd for X and Y, so X/Y can be reduced to lowest terms $\left(\frac{X}{T}\right) / \left(\frac{Y}{T}\right)$. Now the set of divisors of $\frac{X}{Z}$ (resp., $\frac{Y}{Z}$) is $\left\{uZ^n, \frac{uX}{Z^{n+1}} \mid u \in k^*, n \geq 0\right\}$ *(resp.,* $\left\{uZ^n, \frac{uY}{Z^{n+1}} \mid u \in k^*, n \geq 0\right\}$*).* So any common divisor of $\frac{X}{Z}$ and $\frac{Y}{Z}$ is of the form uZ^n where $n \geq 0$ and $u \in k^*$. It follows that $\frac{X}{Z}$ and $\frac{Y}{Z}$ do not have a weak gcd in D and hence $\left(\frac{X}{Z}\right) / \left(\frac{Y}{Z}\right)$cannot be reduced to lowest terms in D. However, $\left(\frac{X}{Z}\right) / \left(\frac{Y}{Z}\right)$ can be put in lowest terms $\left(\frac{X}{T}\right) / \left(\frac{Y}{T}\right)$. It is interesting to note that in the localization $D[T^{-1}]$ of D, X/Y cannot be put in lowest terms.

Now LT domains and weak GCD domains were introduced in [3] in the context of atomic factorization. Let D be an integral domain. Then a nonzero nonunit element a of D is *irreducible*, or an *atom*, if $a = bc$ for $b, c \in D$ implies b or c is a unit. And D is *atomic* if every nonzero nonunit of D is a finite product of atoms. It is well known that if D satisfies ACCP, then D is atomic, but the converse is false. It is easily shown that if D satisfies ACCP, then so does $D[X]$. This raised the question of whether D atomic implies $D[X]$ is atomic which was answered in the negative in [6]. (It is easy to see that if $D[X]$ satisfies ACCP (resp., is atomic), then D satisfies ACCP (resp., is atomic)). Recall that an integral domain D is *strongly atomic* if for $a, b \in D^*$, there exist atoms $a_1, \ldots, a_s (s \geq 0)$ and $c, d \in D^*$ with $[c, d] = 1$ and $a = a_1 \cdots a_s c$ and $b = a_1 \cdots a_s d$. Note that D satisfies ACCP $\Rightarrow$ $D[X]$ is atomic $\Rightarrow$ D is strongly atomic. The following result links these various concepts.

Theorem 3 *For an integral domain D the following are equivalent.*

1. *D is an atomic RLT domain.*
2. *D is an atomic weak GCD domain.*
3. *D is strongly atomic.*
4. *Every linear polynomial in $D[X]$ is a product of atoms.*

Proof (1)⇔(2) Theorem 1 (2). (2)⇒(3) Let $a, b \in D^*$. So D a weak GCD domain gives $a = a'c, b = b'c$ where $[a', b'] = 1$. Since D is atomic, either c is a unit or c is a product of atoms.

(3)⇒(4) Let $aX + b \in D[X]$ be a linear polynomial, so $a \in D^*$. Suppose $b \neq 0$. Then $a = a_1 \cdots a_s c$ and $b = a_1 \cdots a_s d$ where the a_i's are atoms ($s \geq 0$) and $[c, d] = 1$, $c, d \in D^*$. Then $aX + b = a_1 \cdots a_s(cX + d)$ is a product of atoms. So suppose $b = 0$. Then aX is a product of atoms if and only if a is, so it suffices to show that D is atomic, i.e., strongly atomic ⇒ atomic. Let $a \in D^*$ be a nonunit. Write $a = a_1 \cdots a_s c$ and $a^2 = a_1 \cdots a_s d$ where $[c, d] = 1$. Then $a_1^2 \cdots a_s^2 c^2 = a^2 = a_1 \cdots a_s d$. So canceling gives $d = a_1 \cdots a_s c^2$. Thus $c|d$ and hence c is a unit. So a is a product of atoms.

(4)⇒(2) For a nonunit $a \in D^*$, aX a product of atoms implies a is a product of atoms, so D is atomic. For $a, b \in D^*$, $aX + b$ is a product of atoms, so $aX + b = a_1 \cdots a_s(cX + d)$ where each a_i is an atom and $[c, d] = 1$. Put $e = a_1 \cdots a_s$. So $\left[\frac{a}{e}, \frac{b}{e}\right] = [c, d] = 1$ and hence e is a weak gcd for a and b. (We note that the equivalence of (2) and (3) is given in [3, Theorem 1.3]).

While an integral domain satisfying ACCP is an RLT domain, we next give an example of an atomic domain that is not even an LT domain.

Example 4 (An Integrally Closed Atomic Domain That is Not an LT Domain) Let D be the integral domain $k[X, Y, Z][\{\frac{X}{Z^n}, \frac{Y}{Z^n}\}_{n \geq 1}]$ where k is a field. From Example *1* we have $Z|a$ and $Z|b$ whenever $X/Y = a/b$ for $a, b \in D^*$. Let $A = \mathcal{A}^\infty(D)$ as in [6, Example 5.1]. There it is noted that A is integrally closed and atomic, in fact every reducible element of A is a product of two atoms. It is shown that X and Y do not have a weak gcd, so A is not a weak GCD domain, or equivalently, not an RLT domain. We prove the stronger result that if $X/Y = a/b$ where $a, b \in A$, then $Z|a$ and $Z|b$; so X/Y cannot be put in lowest terms in A. Thus A is not an LT domain. To prove this it suffices to prove the following. Let S be a subring of A containing D with the property that wherever $X/Y = a/b$ for $a, b \in S^*$, then $Z|a$ and $Z|b$. Then for $s \in S^*$ and indeterminate X_s, if $X/Y = a/b$ where $a, b \in S\,[X_s, s/X_s]^*$, then $Z|a$ and $Z|b$. With a change of notation, it suffices to prove the following. Let R be an integral domain and let $a, b \in R^*$. Suppose that $t \in R^*$ has the property that whenever $a/b = c/d$ for $c, d \in R^*$, then $t|c$ and $t|d$. Let $s \in R^*$ and X be an indeterminate over R. Suppose that $a/b = f/g$ for $f, g \in R[X, s/X]^*$. Then $t|f$ and $t|g$. Let $f = \frac{r_n' s^n}{X^n} + \cdots + \frac{r_1' s}{X} + r_0 + r_1 X + \cdots + r_m X^m$ and $g = \frac{t_n' s^n}{X^n} + \cdots + \frac{t_1' s}{X} + t_0 + t_1 X + \cdots + t_m X^m$. Then $a/b = f/g$ gives $ag = bf$. So equating coefficients gives $at_i' s^i = br_i' s^i$ and $at_i = br_i$. If $t_i' \neq 0$ (equivalently $r_i' \neq 0$), then $a/b = r_i'/t_i'$; so $t|r_i'$ and $t|t_i'$. If $t_i' = 0$ (equivalently $r_i' = 0$), then certainly $t|r_i'$ and $t|t_i'$. Likewise, $t|r_i$ and $t|t_i$. Hence $t|f$ and $t|g$.

We next consider the stability of the various types of "lowest terms" domains with respect to certain ring constructions. First, none of the "lowest term" domains except Bezout domains are preserved by homomorphic image. Indeed, for any set of indeterminates $\{X_a\}$, $\mathbb{Z}[\{X_a\}]$ is a UFD, but any integral domain is a homomorphic image of a suitable $\mathbb{Z}[\{X_a\}]$. Also, as a field satisfies all the lowest term properties, none of the various "lowest term" domains are preserved by subrings. Example 4 shows that none of the "lowest term" domains except Bezout domains are preserved by overrings. For $k[X, Y, Z]$ is a UFD while its overring $K[X, Y, Z][\{\frac{X}{Z^n}, \frac{Y}{Z^n}\}_{n\geq 1}]$ is not even an LT-domain. We next show that the LT and RLT properties are not preserved by polynomial extensions. In fact, we give an example of an atomic RLT domain A with $A[X]$ neither atomic nor even an LT domain.

Example 5 (An Atomic RLT Domain A So That $A[X]$ is Neither Atomic Nor an LT Domain) Let D be the integral domain $k[X_1, X_2, X_3, Z][\{\frac{X_1}{Z^n}, \frac{X_2}{Z^n}, \frac{X_3}{Z^n}\}_{n\geq 1}]$ where X_1, X_2, X_3, and Z are indeterminates over the field k. Let $A = \mathcal{A}_{\omega,2}(D)$ as in [6, Example 5.2]. There it is shown that A is an atomic domain, in fact, every nonzero nonunit of A is either irreducible or a product of two irreducibles, and that A is a weak GCD (= RLT) domain. But it is also shown that the polynomial ring $A[X]$ is not atomic and is not a weak GCD domain. Indeed, $X_1X + X_2$, and X_3 do not have a weak GCD in $A[X]$ since X_1, X_2, and X_3 do not have an MCD in A (i.e., an element d with $[\frac{X_1}{d}, \frac{X_2}{d}, \frac{X_3}{d}] = 1$). Thus $A[X]$ is not an RLT domain. We prove the stronger result that if $(X_1X + X_2)/X_3 = a/b$ for $a, b \in A[X]$, then $Z|a$ and $Z|b$; so $(X_1X + X_2)/X_3$ cannot be put in lowest terms. Thus $A[X]$ is not an LT domain. To prove this it suffices to prove the following. Let S be a subring of A containing D with the property that whenever $(X_1X+X_2)/X_3 = a/b$ for $a, b \in S[X]^*$, then $Z|a$ and $Z|b$. Then for any ideal I of S and indeterminate Y over $S[X]$, if $(X_1X+X_2)/X_3 = a/b$ for $a, b \in S[Y, IY^{-1}][X]^*$, then $Z|a$ and $Z|b$. Since $S[Y, IY^{-1}][X] = S[X][Y, IS[X]Y^{-1}]$, it suffices to prove the following. Let R be an integral domain and let $a, b \in R^*$. Suppose that $t \in R^*$ has the property that whenever $a/b = c/d$ for $c, d \in R^*$, then $t|c$ and $t|d$. Let I be a nonzero ideal of R and X an indeterminate over R. Suppose that $a/b = f/g$ for $f, g \in R[X, IX^{-1}]^*$. Then $t|f$ and $t|g$. The proof of this follows mutatis mutandis from the proof given for $f, g \in R[X, s/X]^*$ in Example 4.

Suppose $a, b \in D^*$. We can consider $a, b \in D[X]^*$. As such it is possible to put a/b in lowest terms $f(X)/g(X)$ where $f(X), g(X)$ are positive degree polynomials of $D[X]$; see the paragraph after Theorem 4. However, if a/b is reduced to lowest terms $f(X)/g(X)$ in $D[X]$, then $f(X), g(X) \in D^*$. Thus, if $D[X]$ is an RLT domain so is D. Now $D[X]$ is an "absolute LT domain" if and only if $D[X]$ is Bezout, or equivalently, D is a field. And $D[X]$ is a "strong LT domain", equivalently a GCD domain, if and only if D is a GCD domain, equivalently, a "strong LT domain". We have been unable to determine if $D[X]$ an LT domain implies that D is an LT domain. However, if $D[X]$ is a ULT domain, so is D; in fact, D must be a GCD domain. This is our next theorem.

Theorem 4 *For an integral domain, the following are equivalent:* (1) $D[X]$ *is a ULT domain,* (2) $D[X]$ *is a GCD domain, and* (3) D *is a GCD domain.*

Proof It is well known that (2)⇔(3) and (2)⇒(1) by Theorem 1 (5)(b); so it suffices to show that (1)⇒(3). We first show that D is a ULT domain. Suppose $a, b \in D^*$, so $a/b = f(X)/g(X)$ where $f(X), g(X) \in D[X]^*$ with $[f(X), g(X)] = 1$. Suppose that $\deg f(X) > 0$. Then for each $r \in D, f(X)/g(X) = a/b = f(X - r)/g(X - r)$ and $[f(X-r), g(X-r)] = 1$. We may assume that D is infinite, so there exists an $r_0 \in D^*$ with $f(X)$ and $f(X - r_0)$ not associate. But then $f(X)/g(X)$ and $f(X - r_0)/g(X - r_0)$

are two lowest term representations for a/b, contradicting our assumption that $D[X]$ is a ULT domain. Hence $0 = \deg f(X) = \deg g(X)$. So D is an LT domain and hence a ULT domain. By Theorem 1 (5)(b), to show that D is a GCD domain it suffices to show that D is an RLT domain. Let $a, b \in D^*$; so $a/b = c/d$ where $c, d \in D^*$ with $[c, d] = 1$. Now $a/b = c/d = (c + aX)/(d + bX)$. Since $D[X]$ is a ULT domain, we must have $[c + aX,\ d + bX] \neq 1$. Let $f(X) \in D[X]^*$ be a nonunit divisor of $c + aX$ and $d + bX$. If $\deg f(X) = 0$, then $f(X)$ is a nonunit of D dividing both c and d, a contradiction. So $\deg f(X) = 1$ say $f(X) = \alpha + \beta X$. So $\alpha \mid c$ and $\alpha \mid d$; hence α must be a unit of D, so we can take $\alpha = 1$. Then $c + aX = c(1 + \beta X)$ and $d + bX = d(1 + \beta X)$. Thus $a = c\beta$ and $b = d\beta$. So $a/b = c/d = (\frac{a}{\beta})/(\frac{b}{\beta})$. Thus D is an RLT domain.

Now it is quite possible for $a, b \in D^*$, to have $a/b = f(X)/g(X)$ where $f(X), g(X) \in D[X]^*$ with $[f(X), g(x)] = 1$ and $\deg f(X) = \deg g(X) > 0$. Indeed, suppose that $a/b = c/d = e/f$ where $c, d, e, f \in D^*$ with $[c, d] = 1 = [e, f]$ and c and e are not associates. Then $a/b = (c + eX)/(d + fX)$ where $[c + eX,\ d + fX] = 1$. Suppose that we take $D = k[X^2, X^3]$ as in Example 2. Let T be an indeterminate over D. Then $X^3/X^2 = (X^3 + X^4T)/(X^2 + X^3T)$ where $[X^3 + X^4T,\ X^2 + X^3T] = 1$.

The following diagram shows the relationships among the various integral domains we have discussed. None of the implications can be reversed with the possible exceptions of RLT⇒LT and GCD⇒ULT.

$$\begin{array}{ccccccc}
 & & \text{UFD} & & & & \text{Bezout} \\
 & \swarrow & & \searrow & & \swarrow & \\
\text{ACCP} & & & & \text{GCD} & & \\
\Downarrow & & & \swarrow & & \searrow & \\
\text{strongly atomic} & \Rightarrow & \text{RLT} & & & & \text{ULT} \\
\Downarrow & & & \searrow & & \swarrow & \\
\text{atomic} & & & & \text{LT} & &
\end{array}$$

We end with the following two questions.

Question 1 Must an LT domain be an RLT domain?

Question 2 Must a ULT domain be a GCD domain?

References

1. Anderson, D.D.: GCD domains, Gauss' Lemma, and content of polynomials. In: Chapman, S. Glaz, S. (eds.) Non-Noetherian Commutative Ring Theory. Mathematics and Its Applications, vol. 520, pp. 1–31. Kluwer Academic Publishers, Dordrecht, Boston, London (2000)
2. Anderson, D.D., Quintero, R.: Some generalizations of GCD domains. In: Anderson, D.D. (ed.) Factorization in Integral Domains, pp. 189–195. Marcel Dekker, New York (1997)
3. Anderson, D.D., Anderson, D.F., Zafrullah, M.: Factorization in integral domains. J. Pure Appl. Algebra **69**, 1–19 (1990)

4. Gilmer, R.: Multiplicative Ideal Theory. In: Queen's Papers in Pure and Applied Mathematics, vol. 90. Queen's University, Kingston, ON (1992)
5. Mott, J.L., Zafrullah, M.: On Prüfer v-multiplication domains. Manuscripta Math. **35**, 1–26 (1981)
6. Roitman, M.: Polynomial extensions of atomic domains. J. Pure Appl. Algebra **87**, 187–199 (1993)

Unique Factorization in Torsion-Free Modules

Gerhard Angermüller

Abstract A generalization of unique factorization in integral domains to torsion-free modules ("factorial modules") has been proposed by A.-M. Nicholas in the 1960s and subsequently refined by D.L. Costa, C.-P. Lu and D.D. Anderson, S. Valdes-Leon. The aim of this note is to prove new results of this theory. In particular, it is shown that locally projective modules, flat Mittag-Leffler modules and torsion-free content modules are factorial modules. Moreover, factorially closed extensions of factorial domains are characterized with help of factorial modules.

Keywords Content module • Factorial domain • Factorial module • Inert extension • Locally projective module • Mittag-Leffler module

2000 Mathematics Subject Classification 13C13, 13F15, 13G05

1 Introduction

Unique factorization in integral domains plays a prominent role in algebra. It is explained in many books on basic algebra; moreover, the last decades have seen generalizations of this concept in several directions, see, e.g., [1] and the literature cited there. One of these directions is to introduce various types of factorizations of elements in domains (cf. also [2]); another one is the generalization to commutative rings with zero-divisors (cf. also [3, 4]). Further, in [17], a generalization to torsion-free modules over (factorial) domains has been proposed by A.-M. Nicholas and subsequently refined in [18–20] as well as by Costa [8], by Lu [16], and by Anderson and Valdes-Leon [4].

In this note it is proven that locally projective modules, flat Mittag-Leffler modules, and torsion-free content modules are factorial modules in the sense of Nicholas [17, 18]. Moreover, factorially closed extensions of factorial domains are characterized with the help of factorial modules.

G. Angermüller (✉)
e-mail: gerhard.angermueller@googlemail.com

M. Fontana et al. (eds.), *Rings, Polynomials, and Modules*,
https://doi.org/10.1007/978-3-319-65874-2_2

The content of this paper is organized as follows: In Sect. 2, preliminaries are proven to be used in the following sections; possibly, some of them are of independent interest, e.g. Proposition 1. The basic definitions and properties of factorable modules over commutative domains are contained in Sect. 3. The core of this paper is Sect. 4, where the theory is further developed in the special case of factorial base domains; moreover, in this section it is proven that locally projective modules, flat Mittag-Leffler modules or torsion-free content modules are factorial modules. In Sect. 5 ring extensions are considered which are factorable as modules; in particular, factorially closed extensions of factorial domains are characterized with factorial modules. The last section contains some hints to related literature.

Notation
The basics on (unique) factorization in domains can be found, e.g., in [13, 2.14 and 2.15]; basic concepts of Commutative Algebra used in this note are contained in [5], as well as our standard notation. For more advanced subjects we give detailed references to [6, 7, 11, 12, 14].

In the following sections R denotes a commutative domain with 1, $K = Q(R)$ the field of quotients of R and M a torsion-free R-module. M is identified with its image in $KM := K \otimes_R M$ under the map $1 \otimes id_M$; further, $\widehat{M} := \bigcap \{M_P | P \in Spec(R), ht(P) = 1\} \subseteq KM$. Moreover, $R^\times$ denotes the group of units of R.

2 Preliminaries

In this section we recall some definitions and prove some results to be used in the subsequent sections.

If R is a commutative ring and M an R-module, an element x of R is called a *zero-divisor on* M, if x annihilates some non-zero element of M; M is called *torsion-free*, if $0 \in R$ is the only zero-divisor on M. r, s is called a *(two-element) M-sequence*, if $r, s \in R$, r is not a zero-divisor on M and s is not a zero-divisor on M/rM. M is said to satisfy *accc*, if M satisfies the ascending chain condition on cyclic submodules (or equivalently: any non-empty family of cyclic submodules of M has a maximal element). R is said to satisfy *accp*, if R satisfies the ascending chain condition on principal ideals. A submodule N of M is called *torsion-closed in* M if M/N is torsion-free; N is called *pure in* M, if for all finite families $(x_i)_{i\in I}$, $(y_j)_{j\in J}$, $(r_{ij})_{i\in I, j\in J}$ of elements of N, M and R respectively such that for all $i \in I$, $x_i = \sum_{j\in J} r_{ij} y_j$, there is a family $(z_j)_{j\in J}$ of elements of N such that for all $i \in I$, $x_i = \sum_{j\in J} r_{ij} z_j$. Clearly, any pure submodule of M is torsion-closed in M. M^* denotes the R-module of R-linear forms on M. M is called *torsionless*, if for each $x \in M$ there is a $f \in M^*$ such that $f(x) \neq 0$; M is called *reflexive*, if the canonical homomorphism $m \mapsto (f(m))_{f\in M^*}$ is a bijection from M onto M^{**}. M is called *locally projective*, if for each surjective homomorphism $f : P \to Q$ of R-modules, each R-homomorphism $g : M \to Q$ and each finitely generated submodule N of M there is an R-homomorphism $h : M \to P$ such that $f \circ h(x) = g(x)$ for all $x \in N$; obviously, any projective module is locally projective. M is called a *content module*, if for every family $(I_\lambda)_{\lambda\in\Lambda}$ of ideals I_λ of R: $\bigcap_{\lambda\in\Lambda}(I_\lambda M) = (\bigcap_{\lambda\in\Lambda} I_\lambda)M$; if $x \in M$ and $(I_\lambda)_{\lambda\in\Lambda}$ is the family of all ideals I_λ of R such that $x \in I_\lambda M$, then $c(x) := \bigcap_{\lambda\in\Lambda} I_\lambda$ is called the *content of* x. M is called a *Mittag-Leffler-module*, if for every family $(Q_i)_{i\in I}$ of R-modules, the canonical map $M \otimes_R \prod_{i\in I} Q_i \to \prod_{i\in I} M \otimes_R Q_i$ is injective.

An element q of a commutative ring R is called an *atom*, if it is non-zero, not a unit and for all $r, s \in R$ such that $q = rs$, either r or s is a unit of R; q is called *prime*, if qR is a non-zero prime ideal of R. A domain R is called *atomic*, if any non-zero non-unit element of R can be expressed as a finite product of atoms. R is called a *factorial domain* (or a *UFD*), if any non-zero non-unit element of R can be expressed uniquely as a finite product of atoms up to units of R; as is well-known, e.g., by [13, Theorem 2.21], a domain R is factorial if and only if it satisfies accp (resp. is atomic) and every atom of R is prime. R is called a *GCD-domain*, if any two elements of R have a greatest common divisor. By [13, Theorem 2.22], a domain is factorial iff it is a GCD-domain satisfying accp. Concerning *Krull domains*, we refer to [7, Chapter VII].

The following technical argument is used in the proof of [4, Theorem 2.8].

Lemma 1 *Let $M \neq 0$ be such that for each $x \in M$, $x \neq 0$, there is a natural number $j(x)$ so that if $x = r_1 \cdots r_k y$, where r_i $(i = 1, \dots, k)$ is a non-unit of R, and $y \in M$, then $k \le j(x)$. Then R is atomic.*

Proof Choose $m \in M$, $m \neq 0$. Let r be a non-zero non-unit of R. If $r = r_1 \cdots r_k$ is a factorization of r into non-units r_i of R $(i = 1, \dots, k)$, then $k \le j(rm)$ by assumption on M; in particular, there are such factorizations of r with maximal k. By definition of an atom, any factorization $r = r_1 \cdots r_k$ of r into non-units r_i of R $(i = 1, \dots, k)$ with maximal k is in fact a factorization into atoms. □

The following lemma is easily proved and probably known, but we could not find a reference.

Lemma 2 *Let $R \subseteq S$ be a ring extension.*

a) If S is a torsion-free R-module such that $S \cap Q(R) = R$, then $S^\times \cap R = R^\times$.
b) If S is a domain satisfying accp and $S^\times \cap R = R^\times$, then S satisfies accc as R-module.

Proof a) Let $r \in S^\times \cap R$, i.e. $rs = 1$ for some $s \in S$. Then $s = 1/r \in S \cap Q(R) = R$, whence $r \in R^\times$. b) Let $(Rx_i)_{i\in I}$ be any non-empty family of cyclic R-submodules of S. Then $(Sx_i)_{i\in I}$ is a non-empty family of principal ideals of S, whence has a maximal element Sx for some $x = x_j, j \in I$. Rx is a maximal element of $(Rx_i)_{i\in I}$: Let $i \in I$ and $Rx \subseteq Rx_i$. Then $x = rx_i$ for some $r \in R$; by choice of x, $Sx = Sx_i$. If $x = 0$, the assertion is obvious; otherwise, $rs = 1$ for some $s \in S$. Then $r \in S^\times \cap R = R^\times$ and in particular, $Rx = Rx_i$. □

The following assertion is more generally true for arbitrary (weakly) regular sequences, but for the sake of this note, the special case is sufficient.

Lemma 3 *If M is a flat M-module, then any two-element R-sequence is an M-sequence.*

Proof Let r, s be an R-sequence. As M is torsion-free, r is not a zero-divisor on M. Further, multiplication by s on R/rR is injective; as M is flat, multiplication by s on $M/rM \cong R/rR \otimes_R M$ is injective too. □

The following lemma is shown in the proof of [9, Proposition 1.5].

Lemma 4 *If R is a Krull domain, $M = \widehat{M}$ if and only if every two-element R-sequence is an M-sequence.*

Proof First, assume $M = \widehat{M}$. Let r, s be an R-sequence and $x, y \in M$ such that $rx = sy$. Then for any prime ideal P of R of height 1, $(r, s) \not\subseteq P$ (see, e.g., [14, Theorem 132]), i.e. $r \notin P$ or $s \notin P$. In the first case, $y \in M_P = rM_P$; in the second case, $y = r(x/s) \in rM_P$. Thus $y \in \bigcap\{rM_P | P \in Spec(R), ht(P) = 1\} = r\widehat{M} = rM$. Secondly, assume that every two-element R-sequence is an M-sequence and let $x \in \widehat{M}$. Then for every prime ideal P of R of height 1, $(M : x)_P = (M_P : x) = R_P$, whence $(M : x) \not\subseteq P$. Choose $r \in (M : x)$, $r \neq 0$, and denote by $P_1, \ldots, P_n$ the prime ideals of R of height 1 containing r. If $n = 0$, $r \in R^\times$ and thus $x \in M$; so, let us assume $n > 0$. R being a Krull domain, Rr is a decomposable ideal of R [11, Corollary 43.10], whence $\bigcup_{i=1,\ldots,n} P_i$ is the set Z of zero-divisors of R on R/Rr [5, Proposition 4.7]. By the above, $(M : x)$ is not contained in any P_i for $i = 1, \ldots, n$, and hence $(M : x) \not\subseteq Z$ by [5, Proposition 1.11 i)]. Thus we can choose $s \in (M : x) \setminus Z$. Then r, s is an R-sequence, whence an M-sequence by assumption. By choice of r, s: $rx, sx \in M$ and thus $r(sx) = s(rx)$ implies $rx \in rM$, i.e. $x \in M$. □

An extension $R \subseteq S$ of Krull domains is said to satisfy PDE, if for every prime ideal P of S of height 1, the prime ideal $P \cap R$ of R is zero or of height 1 (cf. [7, VII, §1.10]). The following lemma is proven in [9, Proposition 1.5].

Lemma 5 *If R and S are Krull domains, $R \subseteq S$ satisfies PDE if and only if every two-element R-sequence is an S-sequence.*

Proof Observe that in any Krull domain T, any principal ideal I, $0 \neq I \neq T$, has a primary decomposition, whose primary ideals belong to prime ideals of height 1 [11, Corollary 43.10 a)]; in particular, the set of zero-divisors on T/I is a finite union of prime ideals of T of height 1 [5, Proposition 4.7]. Assume first that $R \subseteq S$ satisfies PDE and let r, s be an R-sequence. Further, denote by Z the set of zero-divisors on S/rS; by the above, $Z = P_1 \cup \ldots \cup P_n$ for some height 1 prime ideals P_i of S. If s would be an element of Z, then $r, s \in P_i \cap R$ for some i by [5, Proposition 1.11 i)], whence $P_i \cap R$ would be of height > 1 [14, Theorem 132], contradicting PDE. Thus s is not a zero-divisor on S/rS, that is, r, s is an S-sequence. Assume now that any two-element R-sequence is an S-sequence and let P be a prime ideal of S of height 1; it has to be shown that the height of $P \cap R$ is 0 or 1 . Assuming the contrary, we can choose $r \in P \cap R$, $r \neq 0$ and, by the above, $s \in P \cap R$ such that s is not a zero-divisor on R/rR. Then r, s would be an R-sequence, whence an S-sequence contained in the height 1 prime ideal P, a contradiction [14, Theorem 132]. □

The conditions (3) and (4) of the following proposition are considered in [16, Theorem 2.1].

Proposition 1 *Let R be a factorial domain. The following conditions are equivalent:*

(1) $M = \widehat{M}$
(2) Every two-element R-sequence is an M-sequence
(3) For every prime element p of R, $rx \in pM$ for $r \in R, x \in M$ implies $r \in Rp$ or $x \in pM$.
(4) For all $r \in R$, $x \in M$, the submodule $rM \cap Rx$ is cyclic.

Proof (1)⇔(2) follows by Lemma 4, any factorial domain being a Krull domain. (2)⇒(3): Let p be a prime element of R, $r \in R$ and $x, y \in M$ such that $rx = py$. If p does not divide r, then p, r is an R-sequence, whence an M-sequence and thus $x \in pM$. (3)⇒(2): Let r, s be an R-sequence and $x, y \in M$ such that $rx = sy$. As R is factorial, r and s are relatively prime. We prove by induction on the number n of primes dividing r that $y \in rM$. If $n = 0$, r is a unit in R and the assertion is clear. Let now $n > 0$ and assume the assertion to be true for $n - 1$. Choose a prime element p of R dividing r, i.e. $r = pt$ for some $t \in R$. Then $sy = rx = ptx$, whence $y = pz$ for some $z \in M$ by assumption (3). Thus $psz = sy = ptx$, whence $sz = tx$ and thus $z = tw$ for some $w \in M$ by induction hypothesis. Putting all together, one obtains $y = pz = ptw = rw \in rM$. (3)⇒(4): Let $r \in R$, $x \in M$. We prove by induction on the number n of primes dividing r that $rM \cap Rx$ is cyclic. If $n = 0$, r is a unit in R and $rM \cap Rx = M \cap Rx = Rx$. Let now $n > 0$ and assume the assertion to be true for $n - 1$. Choose a prime element p of R dividing r, i.e. $r = ps$ for some $s \in R$. If $x = py$ for some $y \in M$, then $sM \cap Ry = Rz$ for some $z \in M$ by induction hypothesis, and thus $rM \cap Rx = psM \cap Rpy = p(sM \cap Ry) = Rpz$. If $x \notin pM$, we first observe that $pM \cap Rx = Rpx$: in fact, if $t \in R$, $w \in M$ are such that $pw = tx$, then (by assumption (3)) $t = up$ for some $u \in R$, whence $pw = tx = upx \in Rpx$. Moreover, by induction hypothesis, $sM \cap Rx = Rv$ for some $v \in M$. Then $rM \cap Rx = (rM \cap pM) \cap Rx = rM \cap (pM \cap Rx) = psM \cap Rpx = p(sM \cap Rx) = Rpv$. (4)⇒(3): Let p be a prime element of R, $r \in R$ and $x, y \in M$ such that $rx = py$. By assumption (4), $pM \cap Rx = Rz$ for some $z \in M$; in particular, $rx = py = sz$ for some $s \in R$ as well as $px = tz$ for some $t \in R$. Furthermore, $z = ux = pw$ for some $u \in R$, $w \in M$. If $x = 0$, the assertion is trivially true. If $x \neq 0$, then $px = tz = tux$, whence $p = tu$; as p is prime, either $t \in R^{\times}$ or $u \in R^{\times}$. If $t \in R^{\times}$, then $rx = sz = st^{-1}px$, whence $r = st^{-1}p \in Rp$; if $u \in R^{\times}$, then $x = u^{-1}z = u^{-1}pw \in pM$. □

3 Atomic and Factorable Modules

The following definitions are basic for this note.

Definition 1 Let $x \in M$.

An element $r \in R$ (resp. $m \in M$) is called *an R-divisor* of x (resp. *an M-divisor of* x), if $x = ry$ for some $y \in M$ (resp. $x = sm$ for some $s \in R$); r (resp. m) is called *a greatest R-divisor* (resp. *a smallest M-divisor*) of x, if any R-divisor of x divides r (resp. m is an M-divisor of any M-divisor of x).

x is called *irreducible* if any R-divisor of x is a unit of R.

x is called *primitive* if $x \neq 0$ and x is a smallest M-divisor of any non-zero element of Rx.

M is called *atomic*, if any non-zero element of M has an irreducible M-divisor.

M is called *factorable*, if any non-zero element of M has a smallest M-divisor.

M has the *finite divisor property* (or has *fdp*) if each non-zero element of M has, up to units, only a finite number of proper R-divisors.

A prime element p of R is called *prime for M* if $rx \in pM$ for $r \in R, x \in M$ implies $r \in Rp$ or $x \in pM$.

Remark 1

a) The irreducible elements of R—considered as an R-module—are the units of R. To avoid conflicts, we use the term "atom" for "irreducible elements of a domain" in the sense of [13, Section 2.14].
b) R—considered as an R-module—is atomic and factorable; the primitive elements are the units of R.
c) It is easily checked that the R-module $K = Q(R)$ has irreducible elements if and only if $K = R$; in particular, K is neither atomic nor factorable, if $K \neq R$.
d) If R is a factorial domain, then R has fdp when considered as an R-module; in this case, any prime element of R is prime for R.
e) If R is a field and x is any non-zero element of M, then x is a smallest M-divisor of x: in fact, if $x = ry$, where $r \in R$ and $y \in M$, then $r \neq 0$ and $y = r^{-1}x$. In particular, every vector space is factorable.
f) Let $R := k[X, Y]$ be a polynomial ring in two variables X, Y over a field k and $M := RX + RY$. The irreducible elements of M are the prime elements of the factorial domain R which are contained in M, thus showing, e.g., that the sets of irreducible elements of a module and that of a factorable module containing it can be disjoint (cf. a)). Moreover, M does not have primitive elements: otherwise there would exist an element x of M, $x \neq 0$, such that x is a smallest M-divisor of xX as well as of xY, i.e. a divisor of X and of Y, a contradiction to $M \neq R$. A similar argument shows that the element XY of M does not have a smallest divisor in M, thus proving that the submodule M of the factorable module R is not factorable. As M is a submodule of R, it has fdp too (cf. d); in Remark 3 there is an example of a module having fdp which is not a submodule of a factorable module.

More elementary facts related to Definition 1 are contained in the following lemma:

Lemma 6

a) *Greatest R-divisors (resp. smallest M-divisors) of any non-zero element of M are uniquely determined up to units of R.*
b) *Let $m, x \in M$, $r \in R$, $x \neq 0$ such that $x = rm$. Then r is a greatest R-divisor of x if and only if m is a smallest M-divisor of x.*
c) *A smallest M-divisor of any non-zero element of M is irreducible.*
d) *Every primitive element of M is irreducible.*
e) *If $m, n \in M$ are primitive and $r, s \in R$, $r, s \neq 0$ are such that $rm = sn$, then $m = un$ and $s = ur$ for some $u \in R^\times$.*
f) *For every $x \in M$ the following assertions are equivalent:*

(1) *x is primitive*
(2) *$x \neq 0$ and $Kx \cap M = Rx$*
(3) *Rx is a maximal rank 1 submodule of M*
(4) *$x \neq 0$ and Rx is torsion-closed in M*
(5) *$x \neq 0$ and for every $y \in M$ either $Rx \cap Ry = 0$ or $Ry \subseteq Rx$*
(6) *$x \neq 0$ and for every $r \in R$, $r \neq 0$, r is a greatest R-divisor of rx.*

Proof a): Let $x \in M$, $x \neq 0$. If $r, s \in R$ (resp. $m, n \in M$) are greatest R-divisors (resp. smallest M-divisors) of x, then r divides s (resp. m is an M-divisor of n) and vice versa. In any case, by the assumption on R and M, r and s (resp. m and n) differ by units of R. b) follows immediately from the definitions. c): Let $x \in M$, $x \neq 0$. Let $m \in M$ be a smallest M-divisor of x and let $r \in R$ and $n \in M$ be such that $m = rn$. By assumption on m, m is an M-divisor of n , whence r is a unit of R. d) follows from c). e) follows from the definition of primitive elements and a). f): Let $x \in M$. (1)$\Rightarrow$(2): If x is primitive and $(r/s)x = y$ for some $y \in M$ and some $r, s \in R$, $s \neq 0$, then $rx = sy$, whence $y = tx$ for some $t \in R$ and thus $r = st$ and $y = (r/s)x = tx \in Rx$. (2)$\Rightarrow$(3): Let N be a rank 1 submodule of M such that $Rx \subseteq N$. As $x \neq 0$ by assumption (2), one has $KN = Kx$ and thus $N \subseteq KN \cap M = Kx \cap M = Rx$. (3)$\Rightarrow$(4): Let $r, s \in R$, $r \neq 0$ and $y \in M$ be such that $ry = sx$. Then $y = 0 \in Rx$ or $Ky = Kx$ and thus $Rx \subseteq Ky \cap M$, whence $Ky \cap M = Rx$ by assumption (3); in particular, $y \in Rx$. (4)$\Rightarrow$(5): Let $y \in M$ and assume that there are $r, s \in R$ such that $rx = sy \neq 0$. By assumption (4), $y \in Rx$ and thus $Ry \subseteq Rx$. (5)$\Rightarrow$(1): Let $r, s \in R$, $r \neq 0$ and $y \in M$ be such that $rx = sy$. Then $Rx \cap Ry \neq 0$ and by assumption, $Ry \subseteq Rx$, whence x is an M-divisor of y. (1)$\Leftrightarrow$(6) follows from b). □

Lemma 7

a) *If M is factorable, then M is atomic.*
b) *If M satisfies accc, then any submodule of M is atomic.*
c) *If M is atomic (resp. factorable), then any torsion-closed submodule of M is atomic (resp. factorable); in particular, if M is atomic (resp. factorable), then any pure submodule of M is atomic (resp. factorable).*
d) *If $M = Rm$ is free of rank 1, then M is factorable; more precisely, m is a smallest M-divisor of any element of M and $R^\times m$ is the set of irreducible (resp. primitive) elements of M.*

Proof a) follows from Lemma 6 c). b): Assuming the contrary, a strictly ascending infinite chain of cyclic submodules of M can be easily constructed. c): Clearly, any irreducible (resp. smallest) M-divisor of any non-zero element of a torsion-closed submodule N of M is an N-divisor and is obviously irreducible in N too (resp. a smallest N-divisor). d) follows from the definitions (and Lemma 6 d)). □

The following proposition and its corollaries give some indication of the usefulness of factorable modules.

Proposition 2 *The following conditions are equivalent:*

(1) M is factorable
(2) Every non-zero element of M has a greatest R-divisor
(3) Every non-zero element $x \in M$ has a representation $x = ry$ with $r \in R$, y an irreducible element of M and this representation is unique up to a unit of R
(4) M is atomic and every irreducible element of M is primitive
(5) Every non-zero element of M has a primitive M-divisor
(6) Every non-zero element $x \in M$ has a representation $x = ry$ with r a greatest R-divisor of x and y a primitive M-divisor
(7) Every maximal rank 1 submodule of M is free.

Proof (1)⇔(2) follows from Lemma 6 b). (1)⇒(3): The first part of (3) follows from Lemma 6 c). Let $x \in M$, $x \neq 0$ be such that $x = ry = sz$ with $r, s \in R$ and irreducible elements y, z of M. Choose a smallest M-divisor w of x; then $y = ew$ and $z = fw$ with $e, f \in R^{\times}$. Further, $u := e^{-1}f \in R^{\times}$ and $r = us, z = uy$. (3)⇒(4): By the first part of (3), M is atomic. To prove the second part of (4), let $x \in M$ be irreducible and $r, s \in R, y \in M$ be such that $rx = sy$. Let $y = tz$ with $t \in R$ and $z \in M$ irreducible. By assumption, $r = ust, z = ux$ for some $u \in R^{\times}$, whence $y = tux$ showing x primitive. (4)⇒(5) is clear from the definition. (5)⇒(6): by assumption, x has a representation $x = ry$ with $r \in R$ and y a primitive M-divisor. By definition, y is a smallest M-divisor of x, whence the assertion follows by Lemma 6 b). (6)⇒(7): let N be a maximal rank 1 submodule of M. Choose $n \in N, n \neq 0$ and $r \in R, x \in M$ primitive such that $n = rx$. Maximality of N implies $N = KN \cap M$. In particular, $x = r^{-1}n \in N$, whence $Rx \subseteq N$ and thus $Rx = N$ by Lemma 6 f) (1)⇒(3). (7)⇒(1): let $x \in M, x \neq 0$. Then $Kx \cap M$ is a maximal rank 1 submodule of M; by assumption, $Kx \cap M = Ry$ for some $y \in Kx \cap M$. By Lemma 6 f) (3)⇒(1), y is primitive in M, whence a smallest divisor of x. □

Proposition 2 (7)⇒(1) yields another proof that any vector space is factorable (cf. Remark 1, e)). The next two corollaries shed some light upon modules of rank 1 and factorability:

Corollary 1 *If M has rank 1, then M is factorable if and only if M is free.*

Proof One direction by Proposition 2, (1)⇒(7), and the other by Lemma 7 d). □

Remark 2 An immediate consequence of Corollary 1 is that every non-principal ideal of any domain R is not factorable, although R is so (cf. Remark 1 b), f)).

Corollary 2 *If M is factorable, every non-zero cyclic submodule N of M is contained in a unique maximal rank 1 submodule of M, and this submodule is free.*

Proof Let $N = Rx$ for some $x \in M, x \neq 0$. By Proposition 2 (1)⇒(5), x has a primitive M-divisor y, i.e. $Rx \subseteq Ry$ and Ry is a maximal rank 1 submodule of M by Lemma 6 f) (1)⇒(3). If N is contained in a maximal rank 1 submodule N' of M, then $N' = Rz$ for some $z \in M$ by Proposition 2 (1)⇒(7) and z is primitive by Lemma 6 f) (3)⇒(1). As $x \in Ry \cap Rz$, one has $Ry = Rz$ by Lemma 6 f) (1)⇒(5). □

Corollary 3 *If M is factorable, then every R-sequence r, s is an M-sequence.*

Proof Let $x, y \in M$ be such that $rx = sy$. Then $x = r'u, y = s'v$ for some $r', s' \in R$ and some primitive elements u, v of M by Proposition 2 (1)⇒(6). This implies $rr'u = ss'v$, whence $rr't = ss'$ for some $t \in R^\times$ by Lemma 6 e). As r, s is an R-sequence, this yields $s' \in Rr$ and thus $y \in rM$. □

Corollary 4 *Let R be a Noetherian integrally closed domain and M a finitely generated factorable R-module. Then M is reflexive.*

Proof If M is factorable, then $M = \widehat{M}$ by Corollary 3 and Lemma 4. As M is finitely generated and R a Noetherian integrally closed domain, M is reflexive by [7, VII, §4.2, Theorem 2]. □

Corollary 5 *If M is factorable and $M \neq 0$, then:*

a) For all $r, s \in R$: $rM \subseteq sM$ if and only if s divides r.
b) For all $r \in R$: $rM = M$ if and only if $r \in R^\times$.
c) For every greatest divisor r of a non-zero element x of M and for every $s \in R$, sr is a greatest divisor of sx.

Proof a): Let $r, s \in R$ be such that $rM \subseteq sM$. By Proposition 2, (1)⇒(5), there is a primitive element x of M; in particular, $rx = sy$ for some $y \in M$. By Lemma 6 b), r is a greatest R-divisor of sy, whence s divides r. b) follows immediately from a). c): Let $y \in M$ be such that $x = ry$. By Lemma 6 b),c), y is irreducible, whence a primitive element of M by Proposition 2, (1)⇒(4). Thus y is a smallest divisor of $sx = sry$ and the assertion follows by Lemma 6 b). □

The next result shows that in general, factorable modules are far away from containing divisible modules. If R is not a field, it shows in particular that any torsion-free R-module containing $K = Q(R)$ as a submodule is not factorable.

Corollary 6 *If M is a factorable module containing an element $x \neq 0$ which has every non-zero element of R as R-divisor, then R is a field.*

Proof By Proposition 2 (1)⇒(2), x has a greatest R-divisor t. By assumption, t^2 divides t, whence $t \in R^\times$. As by assumption, any non-zero element of R divides t, $R \setminus 0 \subseteq R^\times$, i.e. R is a field. □

Factorability of modules have consequences for the base ring:

Corollary 7 *R^2 is factorable if and only if R is a GCD-domain. In particular, if R satisfies accp, R^2 is factorable if and only if R is factorial.*

Proof Let $r, s, t \in R$. It is easily seen that t is a greatest R-divisor of $(r, s) \in R^2$ if and only if t is a greatest common divisor of r and s. Thus the first assertion follows from Proposition 2 (1)⇔(2), the second from [13, Thm. 2.22]. □

Corollary 8 *If M is factorable and R satisfies accp, then M satisfies accc.*

Proof Let $(Rx_i)_{i\in I}$ be any non-empty family of cyclic submodules of M. By Proposition 2 (1)⇒(5), for each $i \in I$, $x_i = s_i y_i$ for some $s_i \in R$ and primitive $y_i \in M$. Then $(Rs_i)_{i\in I}$ is a non-empty family of principal ideals of R, whence has a maximal element Rs_j for some $j \in I$. Then $Rx_j = Rs_j y_j$ is a maximal element of $(Rx_i)_{i\in I}$: let $i \in I$ and $Rx_j \subseteq Rx_i$. Then $x_j = rx_i$ for some $r \in R$, whence $s_j y_j = rs_i y_i$. If $s_j = 0$, the assertion is clear; otherwise, $s_j = trs_i$, $y_i = ty_j$ for some $t \in R^\times$ by Lemma 6 e). By choice of j, $Rs_j = Rs_i$, whence $r \in R^\times$ and thus $Rx_j = Rx_i$. □

Corollary 9 *If M is factorable and R satisfies accp, then any submodule of M is atomic.*

Proof Immediate by Corollary 8 and Lemma 7 b). □

If M is factorable, then M is atomic (by Proposition 2) and every two-element R-sequence is an M-sequence (by Corollary 3). In case of GCD-domains there is a converse:

Corollary 10 *Let R be a GCD-domain. If M is atomic and every two-element R-sequence is an M-sequence, then M is factorable.*

Proof By Proposition 2 (4)⇒(1), it is sufficient to prove that every irreducible element of M is primitive. Let $x \in M$ be irreducible and $y \in M$, $r, s \in R \setminus 0$ be such that $rx = sy$. Let d be a greatest common divisor of r, s; then $r = r'd$, $s = s'd$ for some relatively prime elements $r', s' \in R$. Moreover, $r'x = s'y$ and s', r' is an R-sequence; by assumption, s', r' is an M-sequence, whence s' is an R-divisor of x. As x is irreducible, $s' \in R^\times$ and x is an M-divisor of y. □

4 Factorable Modules over Factorial Domains

The next definition reflects a straightforward approach to the generalization of UFDs to modules, cf. [17–20]. The subsequent propositions and its corollaries explain the role of factorial domains in this context.

Definition 2 M is called *factorial*, if $M \neq 0$ and every non-zero element x of M has a representation $x = r_1 \cdots r_n y$ with atoms r_i $(i = 1, \ldots, n)$ of R, y an irreducible element of M and this representation is unique up to units of R; that is, if $x = s_1 \cdots s_m z$ is another representation with atoms s_i $(i = 1, \ldots, m)$ of R and an irreducible element z of M, then $n = m$, there are units $u_i, u \in R^\times$ and a permutation σ of $\{1, \ldots, n\}$ such that $r_i = u_i s_{\sigma(i)}$ $(i = 1, \ldots, n)$ and $y = uz$.

Proposition 3 *The following conditions are equivalent:*

(1) M is factorial
(2) R is atomic and M is factorial
(3) R is a factorial domain, $M \neq 0$ and M is factorable

(4) $M \neq 0$ *and every non-zero element* x *of* M *has a representation* $x = r_1 \cdots r_i y$ *with atoms* $r_1, \ldots, r_i$ *of* R *and an irreducible element* y *of* M*; moreover, every atom of* R *is a prime element of* R *and every irreducible element of* M *is primitive*

(5) $M \neq 0$ *and every non-zero element* x *of* M *has a representation* $x = r_1 \cdots r_i y$ *with atoms* $r_1, \ldots, r_i$ *of* R*,* y *a primitive element of* M *and this representation is unique up to units of* R*.*

Proof (1)⇒(2): To prove that R is atomic, it suffices to show that M satisfies the assumptions of Lemma 1. Let $x \in M$, $x \neq 0$, and $x = r_1 \ldots r_k y$ with non-units $r_1, \ldots, r_k$ of R and $y \in M$. Further, by (1), write $x = s_1 \cdots s_m z$ with atoms s_i ($i = 1, \ldots, m$) of R and an irreducible element z of M; $j(x) := m$ is independent of the choice of atoms s_i ($i = 1, \ldots, m$) of R and irreducible element z of M. We prove now: $k \leq j(x)$. By (1), $r_k y = r_{k,1} \cdots r_{k,m_k} y_{k-1}$ with atoms $r_{k,1}, \ldots, r_{k,m_k}$ of R and an irreducible element $y_{k-1}$of M. It follows $m_k \geq 1$; otherwise, $r_k y = y_{k-1}$ would be irreducible, i.e. r_k a unit of R, a contradiction. Continuing similarly with $r_{k-1} y_{k-1}$ etc., we obtain a representation of $x = r_1 \cdots r_k y = r_1 \cdots r_{k-1} r_{k,1} \cdots r_{k,m_k} y_{k-1} = r_{1,1} \cdots r_{1,m_1} \cdots r_{k-1,1} \cdots r_{k-1,m_{k-1}} r_{k,1} \cdots r_{k,m_k} y_1$ with atoms $r_{1,1}, \ldots, r_{k,m_k}$ of R, an irreducible element y_1 of M and $m_j \geq 1$ for $j = 1, \ldots, k$. Thus $k \leq \sum_{j=1}^{k} m_j = j(x)$ by assumption (1). (2)⇒(3): As $M \neq 0$, M contains an irreducible element m. R is a factorial domain: by assumption (2), any non-zero element r of R has a factorization into atoms and this factorization is unique up to units of R, because that is the case for the element rm of M. M is factorable by Proposition 2 (3)⇒(1). (3)⇒(4) follows from basic properties of factorial domains and Proposition 2 (1)⇒(3), (4). (4)⇒(5) is clear. (5)⇒(1) follows by Lemma 6 d). □

Proposition 4 *Let* R *be a factorial domain. The following conditions are equivalent:*

(1) M *is factorable*

(2) M *is a submodule of a factorable* R*-module and every two-element* R*-sequence is an* M*-sequence*

(3) M *has fdp and every two-element* R*-sequence is an* M*-sequence*

(4) M *satisfies accc and every two-element* R*-sequence is an* M*-sequence*

(5) M *is atomic and every two-element* R*-sequence is an* M*-sequence.*

Proof (1)⇒(2) follows by Corollary 3. (2)⇒(3) by Proposition 2 (1)⇒(2) and the fact that R is factorial. (3)⇒(4) by definition of accc. (4)⇒(5) by Lemma 7 b). (5)⇒(1) by Corollary 10. □

The condition “every two-element R-sequence is an M-sequence” has some remarkable equivalencies, cf. Proposition 1.

Corollary 11 *Let* R *be a factorial domain and* M *be a flat* R*-module. Then the following conditions are equivalent:*

(1) M *is factorable*

(2) M *is a submodule of a factorable* R*-module*