GAUSS' LEMMA AND VALUATION THEORY

P. N. ÁNH AND M. F. SIDDOWAY

Abstract. Gauss' Lemma is not only critically important in showing that polynomial rings over unique factorization domains retain unique factorization; it unifies valuation theory. It figures centrally in Krull's classical construction of valued fields with pre-described value groups, and plays a crucial role in our new short proof of the Ohm–Jaffard-Kaplansky theorem on Bezout domains with given lattice-ordered abelian groups. Furthermore, Eisenstein's Criterion on the irreducibility of polynomials as well as Chao's beautiful extension of Eisenstein's Criterion over arbitrary domains, in particular over Dedekind domains, are also obvious consequences of Gauss' lemma.

1. Basic notions, preliminary results

The study of the integers under multiplication together with GCD and LCM led to the study of lattice-ordered abelian groups. A group is *lattice-ordered* if it is also a *lattice*, i.e., a set endowed with two binary operations $\wedge$(GCD) and $\vee$(LCM), called *meet* and *join* satisfying $a \wedge (a \vee b) = a = a \vee (a \wedge b)$ for any two elements a, b such that the multiplication is distributive on both meets and joins. Lattice-ordered groups can be characterized as partially ordered groups such that any two elements have both infimum and supremum. Examples for lattice-ordered abelian groups are the additive group of integers with the usual order and the multiplicative group of positive rationals with the partial ordering given by *divisibility*, i.e., $a \leq b$ iff $b = na$ for some natural number n. The first example is also an example of an *ordered group* or a *valuation group*, i.e., of a lattice-ordered group where any two elements are comparable. The *positive cone* of a lattice-ordered abelian group G under addition is the set $P = \{a \in G | a \wedge 0 = 0\}$. Hence $-P \cap P = 0$ holds and so P is a cancellative lattice-ordered monoid with the unique invertible element 0. Moreover, the partial order on P is *natural* in the sense that $a \leq b$ iff $b = a + x$ with $x = b - a \in P$. Each of P and G determines the other uniquely: P is the positive cone of G which is the quotient group of P via subtraction. Lattice-ordered abelian groups are subgroups of vector spaces over rationals, i.e., torsion free. Any submonoid X of a torsion free group G satisfying $-X \cap X = 0$ can be extended to the positive cone making G an ordered group. Positive cones of lattice-ordered abelian groups appear naturally in the study of divisibility in classical number rings. Their study led to several important classes of domains like PIDs, UFDs, Dedekind and Prüfer domains,

Date: February 28, 2015.

2000 *Mathematics Subject Classification.* Primary 13A05, 13D05, 13F05, Secondary 06F05.

Key words and phrases. Bezout domains, Gauss's lemma, lattice ordered groups.

The first author was partially supported by the Hungarian National Foundation for Scientific Research grants no. K-101515, Colorado College during his stay at Colorado College in the Summer of 2012 as well as Vietnamese Institute of Advanced Study in Mathematics (VIASM) and Vietnamese Institute of mathematics.

The second author was supported as the Verner Z. Reed Professor of Natural Science at Colorado College from 2007 to the present.

as well as valuation domains which naturally arise from valuation theory. For details on lattice-ordered groups and divisibility theory of domains we refer to the books [9], [10] and [13]. Recent developments in the divisibility of rings can be found in papers [1], [2] and the forthcoming [3].

2. Gauss' Lemma and Valuation theory

The *divisibility theory* of a commutative ring (domain) is the monoid of (non-zero) principal ideals partially ordered by inverse inclusion, i.e., by divisibility. This is the positive cone of a lattice-ordered abelian group when the ring is a valuation domain or UFD. Therefore the map sending an element to its principal ideal, is a valuation in the following sense.

Definition 2.1. Let F be a field and G a lattice-ordered group together with the extra greatest element ∞ (whence $g + \infty = \infty = \infty + \infty$.) F is called a *(global) valued field* with values in G if there is a surjective map $\| \ \| : F \to G \cup \infty$ such that

(1) $\|a\| = \infty \iff a = 0$
(2) $\|ab\| = \|a\| + \|b\|$ holds for any two elements $a, b \in F$.
(3) $\|a + b\| \geq \|a\| \wedge \|b\|$

By this definition, as an obvious consequence of Gauss' Lemma that products of primitive polynomials are again primitive, a valuation of a UFD can be extended naturally to the field of its rational functions without changing the value group. Recall that the *content* of a polynomial in one variable over a UFD is a GCD of its nonzero coefficiennts and a valuation of a UFD maps naturally a nonzero element to the associated element of the free abelian group generated on the set of prime principal ideals partially ordered in the obvious way. Moreover, continueing this idea, one can define a canonical map from the polynomial ring $A[x]$ or from the power series ring $A[[x]]$ sending an element to the degree of the smallest power of x with a nonzero coefficient. Thus, elements of A map to 0 and the fact that polynomial ring or power series ring over a domain are domains, says that these canonical maps are exactly valuations. It is obvious to ask about extensions of a valuation to an algebraic field extension. To illustrate the subtle circumstances that can arise in the case of algebraic extensions, one can consider the settings of the Gaussian integers and $\mathbb{Z}[\sqrt{-5}]$. The first is a principal ideal domain and the second is a (proper) Dedekind domain. In the first case, there are integral primes which are no longer primes as Gaussian integers, i.e., no longer free generators in the value group. In the second case, the valuation map is not surjective because the free generators are prime ideals which are, in general, not principal. Moreover, in both cases, the degree of the extension is 2 over $\mathbb{Q}$. This suggests that the extension problem is of interest even in the case of quadratic number fields. It is also interesting to ponder an appropriate framework for valuations of rings with zero-divisors, i.e., to search for appropriate value monoids and requirements on valuation maps.

Krull's valuation theory established a dictionary between valued fields and ordered abelian groups. This dictionary was extended later by the Jaffard-Ohm-Kaplansky Theorem between Bezout domains and lattice-ordered abelian groups. In both cases, the proofs are essentially verifications of Gauss' Lemma.

In the rest of this note G is a lattice-ordered abelian group with positive cone P and K is an arbitrary field. Since P is a lattice-ordered monoid, one can use the combined language of both ring theory and partial orders. A subset F of P is a *filter* if it is closed under meets,

and $b \in F$ whenever $a \leq b, a \in F$. Hence filters are ideals in the classical sense, but the converse is not necessarily true. For example, the positive cone of the multiplicative group of positive rationals is the monoid of positive integers where the set of multiples of either 3 or 5 is an ideal, but not a filter.

If we identify the elements $g \in G$ with the symbol X^g, then the group algebra KG can be considered as a ring of generalized (Laurent) polynomials $p = \sum k_g X^g$. Recall that the *content* $c(p)$, of an element $p = \sum a_g x^g \in KG$ is the GCD of the power $g \in G$ appearing in the canonical expression of p, and p is called *primitive* if its content is 0, whence p is in particular an element of the monoid algebra KP. The first obvious application of Gauss' Lemma shows a well-known classical result that group algebras of torsion-free abelian groups over fields are domains.

Lemma 2.1. *KG is a domain. In particular, KP is a domain, too.*

Proof. Since G is torsion-free, there exists a total-ordering of G. Denote this ordering by $\prec$. For arbitrary elements

$$p = \sum a_g x^g \neq 0 \neq q = \sum b_h x^h$$

let g_0, h_0 be the smallest (or largest) exponents in $p,\ q$, respectively. Then the coefficient of $x^{(g_0+h_0)}$ is nonzero. □

Remark 2.2. The above proof shows clearly that the usual verification of the fact that both polynomial rings and power series rings over domains are also domains, is a particular case of Gauss' Lemma.

Theorem 2.3 (Gauss' Lemma for valuations)**.** *Products of primitive polynomials in KG are also primitive.*

Proof. Let $p = \sum_{g \in S} a_g x^g$ and $q = \sum_{h \in S} b_h x^h$ be primitive and assume indirectly that pq is not primitive, i.e., $t = c(pq) > 0$. Then t lies in some maximal filter M of P. The complement $P \backslash M$ is closed under addition, for, if $a, b \in P \backslash M$, then by the maximality of the filter M there are $x, y \in M$ with $a \wedge x = 0 = b \wedge y$. Thus for $z = x \wedge y \in M$ one has $a \wedge z = 0 = b \wedge z$ whence $0 = (a \wedge z) + (b \wedge z) = (a + b) \wedge z$, i.e., $a + b$ is not contained in M and thus $P \backslash M$ is closed under addition.

Now, write $p = p_1 + p_2$ where the exponents of p_1 are outside M, and the exponents of p_2 are in M. Similarly write $q = q_1 + q_2$. By primitivity of p, q, both p_1, q_1 are not zero, consequently their product $p_1 q_1$ is also not 0 by Lemma 2.1. Since $pq = p_1 q_1 + r$ where r is a polynomial with exponents in M and the exponents of $p_1 q_1$ are not in M, one obtains that the content $t = c(pq)$ is not contained in M, a contradiction. □

Remark 2.4. The above proof of Theorem 2.3 is exactly the rewriting of the usual proof of the classical Gauss' Lemma in the language of lattice-ordered abelian groups!

As applications we have

Theorem 2.5 (Jaffard–Ohm–Kaplansky)**.** *For a positive cone P of an arbitrary lattice-ordered abelian group G there is a Bezout domain R whose divisibility theory is just P.*

Recall ring is a *Bezout ring* if its finitely generated ideals are principal ideals. Bezout rings are special cases of the so-called *arithmetical rings*, that is, rings whose lattice of ideals

is distributive. Arithmetical domains are *Prüfer domains*, i.e., domains over them finite generated fractionnal ideals are invertible. Theorem 2.5 provides a large class of examples of Bezout domains. The factors of these Bezout domains are examples of Bezout rings with zero-divisors.

Proof. By Theorem 2.3 the set T of all primitive polynomials in the semigroup algebra KP is multiplicatively closed. Let R be the localization $(KP)_T$. Since every element $p \in KP$ can be written as the product of $X^{c(p)}$ with a primitive polynomial by the naturality of the partial order of P, every principal ideal of R is generated by an element $X^s, s \in P$. Consequently, if I is a finitely generated ideal of R, say, with generators $X^{s_1}, \ldots, X^{s_n}$, then by putting $s = \wedge_{i=1}^n s_i$, $s_i = s + t_i$ one has

$$0 = s - s = \bigwedge_{i=1}^{n} s_i - s = \bigwedge_{i=1}^{n} (s + t_i) - s = \bigwedge_{i=1}^{n} (s + t_i - s) = \bigwedge_{i=1}^{n} t_i,$$

whence $\sum_{i=1}^{i=n} X^{t_i}$ is a primitive polynomial. The equalities

$$\sum_{i=1}^{i=n} X^{s_i} = X^s (\sum_{i=1}^{i=n} X^{t_1}) \ \& \ X^{s_i} = X^s X^{t_i} \ \ \forall\, i = 1, \ldots, n$$

imply $I = (X^s)$ showing that R is a Bezout domain whose divisibility theory is obviously order-isomorphic to P. □

Remark 2.6. The naturality of the partial order of P is crucial because it ensures that every polynomial in KP can be written as a product of its content with a primitive polynomial.

Definition 2.2. A polynomial over a commutative ring is *irreducible* if it can not be written as the product of non-zero, non-constant non-invertible polynomials.

Remark 2.7. If $f = gh \in R[x]$ is a factoriztion of f, then the degree of f is obviously the sum of ones of g and h in the case that R is a domain. However, if R has zero-divisors, then it can happen that both the degrees of g and h are greater than one of f. For example, over $\mathbb{Z}_6$ we have $2x = (x+3x^2)(2x)$ and over $\mathbb{Z}_8$ we have $4x^3 = (2x+4x^4)(6x^2+4x^6)$. This observation shows why it is reasonable only to discuss irreducibility of polynomials over domains although Gauss' lemma holds over arbitrary rings. Eisenstein's criterion is stated in Marcus' book [12] for an arbitrary ring and its maximal ideal. As we just noted, the classical proof of Eisenstein's Criterion cannot extended canonically to rings with zero-divisors. Therefore one need eventually new proof to the case of general rings.

However, for domains we have certainly

Theorem 2.8 (Eisenstein's Criterion, Chao's version revisited)**.** *Let $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ be a polynomial with coefficients in a commutative domain R. If there is a prime ideal P of R and $0 \leq k \neq l \leq n$ such that $a_k \notin P; a_i \in P (i \neq k$ but $a_l \notin P^2$ and $f = gh$, then the degree of g or h is at least $|k - l|$. In particular, f is irreducible if $\{k, l\} = \{0, n\}$.*

Proof. If $f = gh; g = b_0 + b_1 x + \cdots + b_m x^m, h = c_0 + c_1 x + \cdots + c_s x^s; n = m + s > m, s \geq 1$, then by passing to polynomials over the domain R/P one obtains that all coefficients of g except one b_u and all coefficients of h except one c_t are contained in P and $u + t = k$ holds.

However, the condition $a_l \notin P^2$ shows $l \geq \min\{u,t\}$ otherwise one has $a_l = \sum_{i=0}^{i=l} b_i c_{l-i} \in P^2$. If $k > l$, then, then one of u or v is at least $k-l$ by $k = u+t$ whence the statement. If $k < l$, then $l-k < l-u < s, l-k < l-s < m$, completing the proof. □

Remarks 2.9. (1) If the prime ideal P in Theorem 2.8 is a principal ideal $P = (p)$ then we obtain the usual form of Eisenstein's Criterion. Eisenstein's Criterion is an immediate and beautiful example that demonstrates the implication of global results from local conditions. Eisenstein's Criterion can be applied effectively to polynomials over Dedekind domains where the unique factorization of prime ideals holds. Sometimes, one can substitute the variable $ax+b$ for x with an appropriate unit a and a constant b getting a new polynomial which admits application of Eisenstein's Criterion. The substitution x^{-1} for x provides a version of Eisenstein's Criterion where the role of the first and last coefficients a_0, a_n are interchanged. For the history of Eisenstein's Criterion we refer to the recent paper of Cox [6].

(2) If R is a UFD, then by using the prime factorization of coefficients (when we know this), one can easily check the applicability of Eisenstein's Criterion. In the general case, let I be the ideal generated by $a_0, a_1, \ldots, a_{n-1}$. If either some power of a_n is in I or $a_0 \in I^2$, then Eisenstein's Criterion is not applicable. Otherwise, at least in principal, one can check Eisenstein's Criterion for each prime ideal P containing I but excluding a_n where such a prime ideal P is ensured by Zorn's Lemma. In particular, Eisenstein's Criterion is a powerful tool for constructing irreducible polynomials.

(3) $2x^2-2x+3$ is an irreducible polynomial over $\mathbb{Z}[\sqrt{-5}]$ but it is reducible over $\mathbb{Q}[\sqrt{-5}]$. Therefore $(2X^2-2x+3)\mathbb{Z}[\sqrt{-5}]$ is not a principal prime ideal. This example demonstrates the usefulness of the extension of Eisenstein's Criterion from unique factorization domains to arbitary rings, in particular to Dedekind domains. Together with the remark above (after Definition 2.1) on the extension of a global valuation to an algebraic field extension, this simple example suggests exciting potential approaches to the classification of prime polynomials over Dedekind domains and even over number rings.

One can naively define the *content* of a polynomial as the ideal generated by its coefficients and call a polynomial *primitive* if its content is the whole ring (see [4], Exercise 2(iv), Chapter I and [11], Exercise 9, Section 1-1). However, as Eisenstein's Criterion indicates, it is more natural to say that a polynomial is *P-primitive* with respect to a prime ideal P, if P does not contain its content. Then the same argument again implies that products of (P)-primitive polynomials are (P)-primitive. It is clear that a polynomial is primitive if it is P-primitive for any prime ideal P. Therefore, using the content as a valuation of the field $Q(x)$ of rational functions over a Dedekind (or even a Prüfer) domain D with the quotient field Q, one can construct a pid (a Bezout domain) $D \subseteq R \subseteq Q(x)$ whose ideal lattice is isomorphic to the ideal lattice of D. In the case of a Bezout ring R, possibly with zero-divisors, every polynomial $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ can be written as a product of a primitive polynomial and its content $c(f)$ if and only if there exist $b_i \in R$ such that $a_i = db_i, i = 0, 1, \ldots, n$ and the b_i generate R. It is well-known (cf. Lemma 4 in [7]) that the latter condition characterizes *Hermite rings*, i.e., rings whose matrices *admit triangular reduction*, that is, to an arbitrary m by n matrix M there exist invertible square matrices $P \in R_n$ and $Q \in R_m$ such that MP

is *triangular* (i.e, elements below the main diagonal are 0) and QM is triangular. Examples for Hermite rings are principal ideal domains and more generally, Bezout domains. Further examples of hermite rings with zero-divisors can be found on [8]. Gauss' Lemma can be reformulated for Hermite rings as follows.

Theorem 2.10 (Gauss' Lemma for Hermite rings)**.** *If S is the divisibility theory of a Hermite ring R, i.e., the multiplicative monoid of principal ideals partially ordered by reverse inclusion, then the valuation map $\| \| : R \to S : a \in R \mapsto \|a\| = aR \in S$ can be extended to a valuation of $R[x]$ with values in S by sending $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ to its content $c(f) \in S$. In particular, primitive polynomials are non-zero-divisors and the ring of quotients of $R[x]$ by inverting primitive polynomials is again a Hermite ring whose principal ideals are generated by elements of R.*

For the proof we note that every $f \in R[x]$ can be written as $f = aF, a \in R, F \in R[x]$ where F is a primitive polynomial ring because R is a Hermite ring. Since products of primitive rings are again primitive, the theorem follows. This new result shows also that the divisibility theory of a Hermite ring can be extended ti the polynomial ring without changing its divisibility theory .

References

1. P. N. Ánh, L. Márki, P. Vámos, Divisibility theory in commutative rings: Bezout semigroups, *Trans. Amer. Math. Soc.*, **364**(8)(2012), 3967–3992.
2. P. N. Ánh, M. Siddoway, Divisibility theory of semi-hereditary rings, *Proc. AMS*, **138**(12), 4231 – 4242.
3. P. N. Ánh, M. Siddoway, Divisibility theory of Bezout rings with one minimal prime ideal, manuscript.
4. M. F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison – Whesley, 1969.
5. H. Chao, A generalization of Eisenstein's Criterion, *Mathematics Magazine* **47** (1974), 158 – 159.
6. David A. Cox, *Why Eisenstein proved the Eisenstein Criterion and why Schönemann discovered it first*, American Mathematical Monthly **118**(1)(2011), 3 – 21.
7. L. Gilman, M. Henriksen, Some remarks about elementary divisor rings, *Trans. Amer. Math. Soc.*, **82** (1956), 362 – 365.
8. L. Gilman, M. Henriksen, Rings of continuous functions in which every finitely generated ideal is principal, *Trans. Amer. Math. Soc.* **82** (1956), 366–391.
9. F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Pure and Applied Mathematics, 211, Marcel Dekker, New York, 1998.
10. P. Jaffard, *Les Systèmes d'Idéaux*, Dunod, Paris 1960.
11. I. Kaplansky, *Commutative rings*, rev. ed., Univ. Chicago Press, 1974.
12. D. A. Marcus, *Number fields*, Springer 1977.
13. J. Močkoř, *Groups of Divisibility*, D. Reidel Publishing Company 1983

Rényi Institute of Mathematics, Hungarian Academy of Sciences, 1364 Budapest, Pf. 127 Hungary

E-mail address: anh@renyi.hu

Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO 80903.

E-mail address: msiddoway@coloradocollege.edu