Theory and Applications of Mathematics & Computer Science

(ISSN 2067-2764, EISSN 2247-6202)
http://www.uav.ro/applications/se/journal/index.php/tamcs

Theory and Applications of Mathematics & Computer Science 6 (1) (2016) 28–50

Quadratic Equations in Tropical Regions

Wolfgang Rump[a,*]

Dedicated to B. V. M.

[a] *Institute for Algebra and Number Theory, University of Stuttgart, Pfaffenwaldring 57, D-70550 Stuttgart, Germany*

Abstract

In this note, the reader is invited to a walk through tropical semifields and the places where they border on "ordinary" algebra. Though mostly neglected in today's lectures on algebra, we point to the places where tropical structures inevitably pervade, and show that they frequently occur in ring theory and classical algebra, touching at least functional analysis, and algebraic geometry. Specifically, it is explained how valuation theory, which plays an essential part in classical commutative algebra and algebraic geometry, is essentially tropical. In particular, it is shown that Eisenstein's well-known irreducibility criterion and other more powerful criteria follow immediately by tropicalization. Some applications to algebraic equations in characteric 1, neat Bézout domains, and rings of continuous functions are given.

Keywords: ℓ-group, projectable, semifield, polynomial, irreducible, Newton polygon, tropical algebra.
2010 MSC: Primary: 12K10, 26A51, 46E25, 14T05, 11C08, 13F30, 13F05.

1. Introduction

Mathematical ideas quite often originate from natural sciences where experiments help to understand what happens behind reality. In chemistry, the usual method to analyse a matter is by heating until the components begin to separate. "Tropical" mathematics did not quite emerge in that way, but at least one of its founders (Imre Simon) was working on it in the sunny regions of Brazil.

To illustrate the basic process, consider the function

$$a +_p b := (a^p + b^p)^{1/p}$$

for positive real numbers a, b. At "room temperature" ($p = 1$), the function $a +_1 b$ is just ordinary addition in $\mathbb{R}$. Now turn on the heating - proceed until $p \to \infty$ to get the real number system to

*Supported by NSFC-project 11271040 "Ordered Algebraic structures and their applications"
Corresponding author
Email address: `rump@mathematik.uni-stuttgart.de` (Wolfgang Rump)

melt. Recall that F. Riesz (Riesz, 1910) made such an experiment already in 1910, which led him to the invention of Lebesgue spaces $L^p(\mathbb{R})$. If p is replaced by the Planck constant $\hbar := \frac{1}{p}$, the limit process $\hbar \to 0$ is known as a *dequantization* (Litvinov, 2006). Indeed, the passage from L^1 to L^∞ bears a certain analogy to the correspondence principle in quantum mechanics (Bohr, 1920).

Now what remains after melting the real number system? For $p = \infty$, ordinary addition $a + b$ in $\mathbb{R}$ turns into $a \vee b := \max\{a, b\}$. The additive group of $\mathbb{R}$ becomes a semigroup, the field $\mathbb{R}$ of real numbers turns into the semifield $\mathbb{R}^+_{\max}$ of *tropical real numbers*, investigated in the 1987 thesis of Imre Simon (Simon, 1987). A remarkable feature of $\mathbb{R}^+_{\max}$ is that its addition is idempotent:

$$a \vee a = a.$$

Thus, if there would exist additive inverses, the whole system would collapse into the zero ring. So is there any reason to regard the elements of $\mathbb{R}^+_{\max}$ as numbers? Before taking up this question seriously, let us content ourselves for the moment with referring back to F. Riesz' early work on L^p-spaces. Here the connection between $p = 1$ and $p = \infty$ is very tight: $L^\infty(\mathbb{R})$ is just the Banach space dual of $L^1(\mathbb{R})$.

Hilbert once placed the number system between the three-dimensional space and the one-dimensional time, saying that numbers are 'two-dimensional'. Such a statement would still have shocked the mathematical community in the days of Euler who called imaginary numbers "impossible" (Euler, 1911). Nowadays, the two-dimensionality is firmly justified by analytical and algebraic reasons, the latter consisting in the algebraic closedness of $\mathbb{C}$. On the other hand, two-dimensionality would not make sense without reference to the base field $\mathbb{R}$ which is "really" fundamental.

In the tropical world, there is no such distinction: the semifield of tropical reals is "algebraically closed". Making this precise is a good exercise and an invitation to be more careful in stating the 'fundamental theorem of algebra'. To be sure, the latter does not mean that *every* complex polynomial has a root - the non-zero constants have to be excluded. This triviality becomes relevant in the wonderland of tropical algebra: there are tropical semifields where (non-constant) linear equations need not be solvable. Roots and solutions of polynomial equations fall apart, and quadratic equations need not be solvable by radicals. On the other hand, every algebraic equation can be reduced to quadratic ones.

In this paper, classical algebra is revisited with regard to tropical structures, and it is shown that they occur at various places. Apart from a revision of semifields of characteristic 1, we add new characterizations for their algebraic closedness (Theorem 6.1). A connection with neat Bézout domains is given in Corollary 2. As a second application, we show that if the semifield of characteristic 1 corresponding to an ℓ-group $\mathscr{C}(X)$ of contiuous functions on a completely regular space X is algebraically closed, the space X must be an F-space, that is, the corresponding ring $C(X)$ of continuous functions is a Bézout ring (Corollary 3).

Another motivation to study semifields of characteristic 1 comes from a recent, highly conjectural branch of arithmetic geometry. Since André Weil sketched his diagonal argument (Weil, 1940, 1941) to tackle the Riemann hypothesis, some research groups eagerly delve under the surface of $\mathbb{Z}$, searching for its "base field" to make $\mathbb{Z}$ (a ring of Krull dimension one) into an algebra over that field (see, e. g., (Connes & Consani, 2010, 2011; Deitmar, 2008; Soulé, 2011)). The way to this non-existing, mysterious, “field” of characteristic 1 inevitably leads through the tropical region. By Proposition 2.2, this hot region is nothing else than the vast and well-developed theory of lattice-ordered abelian groups.

2. The forgotten characteristic

To include the result of a dequantization, we are advised to consider semifields instead of fields. More generally, a *semiring* is an abelian monoid $(A; +, 0)$ with a multiplicative monoid structure $(A; \cdot, 1)$ satisfying the distributive laws and $a \cdot 0 = 0 \cdot a = 0$ for all $a \in A$. If the group of (multiplicatively) invertible elements, the *unit group* $A^\times$, coincides with $A \setminus \{0\}$, we call A a *semi-skewfield*. If, in addition, the multiplicative monoid is commutative, A is said to be a *semi-field*. For example, the above mentioned $\mathbb{R}^+_{\max}$ is a semifield.

A *morphism* in the category of semirings is a map $f: A \to B$ which satisfies

$$\begin{aligned} f(a+b) &= f(a) + f(b), \qquad & f(0) &= 0 \\ f(a \cdot b) &= f(a) \cdot f(b), \qquad & f(1) &= 1. \end{aligned}$$

Like in the category of rings, there is an initial object, the semiring $\mathbb{N}$ of non-negative integers: For any semi-ring A there is a unique morphism $c: \mathbb{N} \to A$. The image of c is the intersection of all sub-semirings of A, the *prime semiring* of A. Similarly, every semi-skewfield A contains a smallest sub-semi-skewfield. If it coincides with A, we call A a *prime semi-skewfield*.

In general, the kernel $\operatorname{Ker} c := \{n \in \mathbb{N} \mid c(n) = 0\}$ is not of the form $\mathbb{N}p$ for some $p \in \mathbb{N}$. For example, $I := \mathbb{N} \setminus \{1, 2, 4, 7\}$ is an ideal of the semiring $\mathbb{N}$ which occurs, e. g., as the grading of a simple curve singulatity (Greuel & Knörrer, 1985). Thus $\mathbb{N}/I$ is a finite semiring with $\operatorname{Ker}(c) = I$. On the other hand, there exist congruence relations on $\mathbb{N}$ which do not come from an ideal, even if A is a semifield. For example, let $\mathbb{B} := \{0, 1\}$ be the semifield with $1 + 1 = 1$. Then $c: \mathbb{N} \twoheadrightarrow \mathbb{B}$ satisfies $c(n) = 1$ for $n \neq 0$. So c has a trivial kernel, while it is far from being a monomorphism.

Note that $\mathbb{B}$ is the prime a sub-semifield of $\mathbb{R}^+_{\max}$. Therefore, we write $a \vee b$ for the addition in $\mathbb{B}$. So $\mathbb{B}$ is a Boolean algebra with $a \wedge b := ab$. The reader will notice that $\mathbb{B}$ can be derived from the prime field $\mathbb{F}_2$ via $a \vee b = a + b + ab$, but not vice versa.

Definition 2.1. We define the *characteristic* $\operatorname{char} A$ of a semiring A to be the smallest integer $p > 0$ with $c(n + p) = c(n)$ for some $n \in \mathbb{N}$. If such an integer p does not exist, we set $\operatorname{char} A := 0$.

In analogy to the theory of skew-fields, we have (cf. (Rump, 2015), Proposition 1)

Proposition 2.1. *Every prime semi-skewfield is a semifield. Up to isomorphism, the prime semi-fields are $\mathbb{Q}^+$, $\mathbb{B}$, and $\mathbb{F}_p$ for rational primes p. In particular, the prime semifields are determined by their characteristic.*

Proof. Let F be a prime semi-skewfield. Assume first that $\operatorname{char} F = 0$. Then $\mathbb{N}$ can be regarded as a sub-semiring of F. Every non-zero $n \in \mathbb{N}$ has an inverse $\frac{1}{n}$ in F which commutes with all elements of $\mathbb{N}$. Hence $\{\frac{m}{n} \mid m, n \in \mathbb{N}, n > 0\}$ is a sub-semifield isomorphic to the positive cone $\mathbb{Q}^+$ of $\mathbb{Q}$.

Now assume that $p := \operatorname{char} F \neq 0$. Then there is an integer $n \in \mathbb{N}$ with $c(n) + c(p) = c(n)$. As this equation holds for almost all n, we can assume that n is a multiple of p. Adding multiples of $c(p)$ on both sides, the equations obtained in this way imply that $c(n) + c(n) = c(n)$. If $c(n) = 0$, then $c(p) = 0$, and the usual argument shows that $c(\mathbb{N}) \cong \mathbb{F}_p$ for a prime p. Otherwise, we obtain $c(1) + c(1) = c(1)$, which yields $c(\mathbb{N}) \cong \mathbb{B}$. □

So the possible prime semifields are

$$\mathbb{Q}^+, \mathbb{B}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \ldots,$$

including the prime fields $\mathbb{F}_p$ and a natural sub-semifield of $\mathbb{Q}$. Note that formally, $\mathbb{Q}^+$ carries more information than $\mathbb{Q}$: The positive cone provides $\mathbb{Q}$ with its natural ordering. Thus, $\mathbb{Q}^+$ connects arithmetic (the semiring $\mathbb{N}$) with algebra and analysis (the ordered field $\mathbb{Q}$ and its completion $\mathbb{R}$), while the newcomer $\mathbb{B}$ bridges the gap between algebra and logic.

Every semifield contains one of the prime semifields according to its characteristic. For fields, this is a well-known piece of algebra. So the question arises how the "logical" semi-skewfields, those containing $\mathbb{B}$, look like. By Proposition 2.1, they are of characteristic 1, which means that they satisfy the equation $1+1 = 1$. Recall that a partially ordered group is said to be *lattice-ordered* or an *ℓ-group* if the partial order is a lattice. For the theory of ℓ-groups, the reader is referred to (Anderson & Feil, 1988; Bigard *et al.*, 1977; Darnel, 1995; Glass, 1999). The commutative case of the following result is due to Weinert and Wiegandt (Weinert & Wiegandt, 1940). Similar ideas have been developed independently by several authors (see (Castella, 2010; Lescot, 2009), and the literature cited there).

Proposition 2.2. *Up to isomorphism, there is a one-to-one correspondence between ℓ-groups and semi-skewfields of characteristic 1.*

Proof. Note first that a semi-skewfield F is of characteristic 1 if and only if $a + a = a$ holds for all $a \in F$. Then it easily checked that

$$a \leqslant b :\Longleftrightarrow a + b = b \tag{2.1}$$

makes F into a $\vee$-semilattice with $a \vee b := a + b$. Furthermore, the distributivity shows that $F^\times$ is an ℓ-group. Conversely, every ℓ-group G can be made into a semi-skewfield $\widetilde{G} := G \sqcup \{0\}$ by adjoining a smallest element 0 with $0a = a0 = 0$ for all $a \in \widetilde{G}$. Since $\widetilde{G}^\times = G$ and $\widetilde{F^\times} = F$, the correspondence is bijective. □

In particular, semifields of characteristic 1 are equivalent to abelian ℓ-groups, and our prime semifield $\mathbb{B}$ corresponds to the ℓ-group of order one. For those who would like to prove the Riemann hypothesis, we should add that $\mathbb{B}$ is not identical with the desperately sought field $\mathbb{F}_1$ - it is still "too big"!

3. Tropical semi-domains

To study field extensions, one has to understand polynomial rings first. Thus, in characteristic 1, we have to deal with polynomials over the semifield $\widetilde{G}$ of an abelian ℓ-group G. For an arbitrary field K, there are many integral domains with quotient field K. If K is an algebraic number field, there is a canonical subring $\mathscr{O}$ - the ring of integers - with quotient field K. Similarly, any semifield $\widetilde{G}$ of characteristic 1 has a canonical sub-semiring $\widetilde{G^-} := G^- \sqcup \{0\}$, where G^- is the negative cone of G. (Since 0 is the smallest element of $\widetilde{G}$, the cone that touches 0 is the negative one.)

Definition 3.1. We define a *semi-domain* to be a commutative semiring A satisfying $ac = bc \Rightarrow a = b$ for $a, b, c \in A$ with $c \neq 0$. We call A *tropical* if there exists an abelian ℓ-group G with $A = \widetilde{G^-}$.

In particular, a semi-domain has no zero-divisors. An intrinsic description of tropical semi-domains is obtained as follows. Recall that a *hoop* (Blok & Ferreirim, 2000) is a commutative monoid H with a binary operation $\rightarrow$ such that the following are satisfied for all $a, b, c \in H$:

$$\begin{aligned} a \rightarrow a &= 1 \\ ab \rightarrow c &= a \rightarrow (b \rightarrow c) \\ (a \rightarrow b)a &= (b \rightarrow a)b. \end{aligned}$$

Every hoop is a $\wedge$-semilattice with respect to the *natural* partial order

$$a \leqslant b \ :\Longleftrightarrow\ \exists\, c \in H : a = cb \iff a \rightarrow b = 1.$$

A hoop is called *self-similar* (Rump, 2008) if it is cancellative. (For an explanation of the terminology and equational characterizations, see (Rump, 2008), Proposition 5.) Every self-similar hoop H has a group of fractions, the *structure group* $G(H)$ of H, which consists of the fractions $a^{-1}b$ with $a, b \in H$.

Proposition 3.1. *Up to isomorphism, there is a one-to-one correspondence between*

(a) *semifields of charatceristic 1,*
(b) *tropical semi-domains,*
(c) *abelian ℓ-groups, and*
(d) *self-similar hoops.*

Proof. The equivalence between (a) and (c) follows by Proposition 2.2, while the equivalence between (b) and (c) is obvious. For an abelian ℓ-group G, we define

$$a \rightarrow b := ba^{-1} \wedge 1$$

for $a, b \in G^-$. By (Rump, 2008), Section 5, this makes G^- into a self-similar hoop with structure group G. Conversely, the structure group $G(H)$ of a self-similar hoop H is an abelian ℓ-group with $G(H)^- = H$ by (Rump, 2008), Proposition 19. □

Note that Proposition 3.1 implies that a self-similar hoop H is a lattice. Explicitly, the join is given by the formula

$$a \vee b = (a \rightarrow b) \rightarrow b$$

which is well known from the theory of BCK algebras (Iséki & Tanaka, 1978).

The concept of Grothendieck group (Lang, 1965) extends to semirings as follows.

Definition 3.2. Let A be a commutative semiring. We define an *ideal* of A to be an additive submonoid I which satisfies

$$a \in A,\ b \in I \implies ab \in I. \tag{3.1}$$

We say that an ideal P is *prime* if $A \smallsetminus P$ is a submonoid of A.

Let I be an ideal of a commutative semiring. Then

$$a \sim b \ :\Longleftrightarrow\ \exists\, c \in I\colon a + c = b + c$$

is an equivalence relation, and it is easily checked that it is a congruence relation. So the equivalence classes form a commutative semiring A/I, the *factor semiring* modulo I. There is also a concept of localization.

Proposition 3.2. *Let P be a prime ideal of a commutative semiring A. There exists a morphism $q\colon A \to A_P$ of semirings with $q(A \smallsetminus P) \subset A_P^\times$ such that every morphism $f\colon A \to B$ of semirings with $f(A \smallsetminus P) \subset B^\times$ factors uniquely through q.*

Proof. Define an equivalence relation on the multiplicative monoid $A \times (A \smallsetminus P)$:

$$(a, b) \sim (c, d) \ :\Longleftrightarrow\ \exists\, s \in A \smallsetminus P\colon ads = bcs. \tag{3.2}$$

Then $x \sim y$ implies $xz \sim yz$ for all $x, y, z \in A \times (A \smallsetminus P)$. So $\sim$ is a congruence relation on $A \times (A \smallsetminus P)$. As usual, we write $\frac{a}{b}$ for the equivalence class of (a, b). So the equivalence classes form a commutative monoid A_P with a morphism $q\colon A \to A_P$ given by $q(a) := \frac{a}{1}$. Moreover, $q(A \smallsetminus P) \subset A_P^\times$. Furthermore, it is easily checked that

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

is well defined and makes A_P into a commutative semiring such that q becomes a morphism of semirings. Now the universal property is straightforward. □

We call A_P the *localization* of A at P. If the zero ideal is prime, the localization at 0 yields the *quotient semifield* $K(A)$ of A.

Note that there are semirings A where 0 is prime, but A is not a semi-domain. For example, let K be a semifield. We define a *(formal) polynomial* to be an expression

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

with $a_i \in K$. If $f \neq 0$, say, $a_n \neq 0$, we call $\deg f := n$ the *degree* of f. Thus, with the usual operations, the formal polynomials make up a semiring $K\langle x \rangle$, and 0 is a prime ideal. To see that $K\langle x \rangle$ need not be a semidomain, consider the case $\operatorname{char} K = 1$, that is, $K = \widetilde{G}$ for an abelian ℓ-group G. Consider two elements $a, b \in G$ with $a \nleqslant b$. Then the two formal polynomials $a \vee bx \vee x^2$ and $a \vee (a \vee b)x \vee x^2$ are distinct. However,

$$(a^2 \vee bx \vee x^2)(a \vee x) = (a^2 \vee (a \vee b)x \vee x^2)(a \vee x),$$

which shows that $\widetilde{G}\langle x\rangle$ fails to be a semi-domain! That is the reason why we speak of *formal* polynomials.

If A is a semidomain, the equivalence (3.2) simplifies to

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc,$$

which implies that all localizations A_P can be regarded as sub-semidomains of $K(A)$.

Example. Let A be a semidomain of characteristic 1. The quotient semifield $K(A)$ is of the form $K(A) = \widetilde{G}$ with an abelian ℓ-group G, and the monoid $A \smallsetminus \{0\} = A \cap G$ is a $\vee$-sub-semilattice. However, $A \cap G$ need not be the negative cone of G. Indeed, this happens if and only if A is tropical. Assume this from now on. By Definition 3.2, an ideal of A is the same as a $\vee$-sub-semilattice which is a downset. So the complement $Q := A \smallsetminus P$ of a prime ideal P of A is a convex submonoid of G^- with the property

$$a \vee b \in Q \implies a \in Q \ \text{ or } \ b \in Q,$$

that is, Q is the negative cone of a prime ℓ-ideal in G (see (Darnel, 1995), Definitions 8.1 and 9.1). In other words, there is a one-to-one correspondence between prime ideals of A and prime ℓ-ideals of G. According to (Darnel, 1995), Proposition 14.3, the prime ideals of A can be identified with the prime filters of the negative cone G^- (with the reverse ordering). Note that the zero ideal of A corresponds to G, the "trivial" prime ℓ-ideal of G, which should not be excluded from the prime spectrum of G.

Definition 3.3. Let K be a semifield. The elements of the quotient semifield $K(x)$ of $K\langle x\rangle$ will be called *rational functions* in x. We write $K[x]$ for the image of the natural map $K\langle x\rangle \to K(x)$ and call the elements of $K[x]$ *polynomials* in x.

4. Divisors in characteristic 1

In classical algebraic geometry, divisors are intimately connected with line bundles, invertible sheaves, linear systems, and embeddings into projective spaces. Therefore, they play a decisive rôle. Here we shall study their behaviour in characteristic 1.

Thus, let G be an abelian ℓ-group. As a lattice, G is distributive. So the elements of G can be regarded as functions on a set. Let us take the simplest case where G satisfies the ascending chain condition. By a theorem of Birkhoff (Birkhoff, 1942), this implies that G is a cardinal sum $G = \boxplus_{p\in P}\mathbb{Z}$ with basis P. (Such ℓ-groups naturally arise as groups of fractional ideals of a Dedekind domain.) So each interval $[a,b] := \{c \in G \mid a \leqslant c \leqslant b\}$ has a composition series $a = c_0 < c_1 < \cdots < c_n = b$ with atomic intervals $[c_i, c_{i+1}] = \{c_i, c_{i+1}\}$. For a diagram

$$\begin{tikzcd}[column sep=small] & a \vee b \arrow[dl, dash] \arrow[dr, dash] & \\ a \arrow[dr, dash] & & b \arrow[dl, dash] \\ & a \wedge b & \end{tikzcd} \tag{4.1}$$

with $a, b \in G$, the intervals $[a \wedge b, a]$ and $[b, a \vee b]$ are said to be *isomorphic*, in analogy with the isomorphism theorem in group theory. *Isomorphism* between intervals is then defined by finite sequences of elementary isomorphisms (4.1). So each pair $a, b \in G$ can be connected by a finite chain $a = c_0, c_1, \ldots, c_n = b$ in G, with atomic intervals $[c_i, c_{i+1}]$ or $[c_{i+1}, c_i]$. If we attach a factor -1 to the intervals of the second type, the total count of isomorphism classes of atomic intervals on such a connecting path merely depends on the pair of endpoints a, b. Regarding the isomorphism classes of atomic intervals as "points", every element $a \in G$ is completely determined by the formal $\mathbb{Z}$-linear combination of points encountered on a path between 0 and a which is independent of the chosen path. For algebraic curves, a formal $\mathbb{Z}$-linear combination of points is called a *divisor*.

In general, there are no atomic intervals. So we have to watch out for a substitute. This naturally leads to the following

Definition 4.1. Let G be a (multiplicative) abelian ℓ-group, and let D be the subgroup of the free abelian group $\mathbb{Z}^{(G)}$ generated by the elements

$$(a \vee b) + (a \wedge b) - a - b$$

with $a, b \in G$. The factor group $\mathrm{Div}(G) := \mathbb{Z}^{(G)}/D$ will be called the group of *divisors* of G. The natural map $G \to \mathrm{Div}(G)$ will be denoted by $a \mapsto [a]$.

In the special case of a noetherian group G, it is clear that the homomorphism $G \to \mathrm{Div}(G)$ is injective. In general, this follows since $G \to \mathrm{Div}(G)$ admits a retraction $\mathrm{Div}(G) \to G$, given by the map

$$n_1[a_1] + \cdots + n_r[a_r] \mapsto a_1^{n_1} \cdots a_r^{n_r}.$$

The retraction is well defined by virtue of the equation

$$(a \vee b)(a \wedge b) = ab,$$

which holds in every abelian ℓ-group. However, even for $G = \mathbb{Z}$, the embedding

$$G \hookrightarrow \mathrm{Div}(G)$$

is far from being surjective. Instead, the group $\mathrm{Div}(G)$ tells us much about the polynomial semi-domain $\widetilde{G}[x]$.

Let $G(x) := \widetilde{G}(x)^\times$ be the abelian ℓ-group which is freely generated by G and a single indeterminate x. Similarly, we set $G[x] := \widetilde{G}[x] \cap G(x)$. The degree of non-zero polynomials extends to a homomorphism

$$\deg\colon G(x) \to \mathbb{Z}.$$

of abelian ℓ-groups. For ordinary fields K, the degree function $\deg\colon K(x)^\times \to \mathbb{Z}$ is also important, but it is not a homomorphism of rings. So the degree of a polynomial or rational function in classical algebra signalizes a tropical structure!

The reader may check that

$$\big(x \vee (a \vee b)\big)\big(x \vee (a \wedge b)\big) = (x \vee a)(x \vee b)$$

holds for all $a, b \in G$. To generalize this fact, recall that an abelian ℓ-group G is *divisible* if every $a \in G$ admits an n-th root for each positive integer n, or equivalently, the pure equation

$$x^n = a$$

is solvable for any $a \in G$. (If G is written additively, this just means that G can be regarded as a $\mathbb{Q}$-vector space.) Now we have ((Rump, 2015), Theorem 1):

Fundamental theorem for abelian ℓ-groups. *Let G be a divisible abelian ℓ-group, and let $K := \widetilde{G}$ be the corresponding tropical semifield. Every non-zero polynomial $f \in K[x]$ has a unique factorization*

$$f = a(x \vee d_1)(x \vee d_2) \cdots (x \vee d_n) \tag{4.2}$$

with $a \in G$ and $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_n$ in K.

For $K = \mathbb{R}^+_{\max}$, this theorem is known as the "fundamental theorem of tropical algebra" (see, e. g., (Cuninghame-Green & Meijer, 1980)). Two things are remarkable. First, the *roots* $d_1 \leqslant \cdots \leqslant d_n$ have to be put into linear order - otherwise, they won't be unique. The roots of a polynomial are in fact nothing else than its divisor. So in contrast to divisors of algebraic curves, tropical divisors are not unique as unordered point sets with multiplicities. For the divisor $[a]+[b]$, the equivalence to $[a \vee b] + [a \wedge b]$ can be seen from the basic relation of Definition 4.1.

Secondly, the roots $d_1 \leqslant \cdots \leqslant d_n$ are not the zeros, because no non-zero polynomial $f \in K[x]$ satisfies $f(a) = 0$ for any $a \in G$. Only equations $f(x) = g(x)$ for a pair of polynomials are sensible! So the question whether polynomial equations can be solved in G is not answered by the fundamental theorem. We will come back to this in Section 5.

By the fundamental theorem, there is a well-defined map

$$\mathrm{div}\colon G[x] \to \mathrm{Div}(G^d) \tag{4.3}$$

for any abelian ℓ-group G with divisible closure G^d, given by

$$\mathrm{div}(f) := [d_1] + [d_2] + \cdots + [d_n]$$

for a non-zero polynomial (4.2). Every rational function $f \in G(x)$ can be written as

$$f = ax^{n_0}(x \vee d_1)^{n_1}(x \vee d_2)^{n_2} \cdots (x \vee d_r)^{n_r} \tag{4.4}$$

with $a, d_1, \dots, d_r \in G$, and $n_0, \dots, n_r \in \mathbb{Z}$. In contrast to polynomials where $n_1, \dots, n_r \in \mathbb{N}$, the d_i cannot be put into linear order, which means that they are not unique! However, a and n_0 are unique. So let $G(x)^0$ denote the subgroup of rational functions $f \in G(X)$ with $a = 1$ and $n_0 = 0$. Then (Rump, 2015), Theorem 2, yields

Theorem 4.1. *Let G be a divisible abelian ℓ-group. The map (4.3) extends uniquely to a group isomorphism*

$$\mathrm{div}\colon G(x)^0 \xrightarrow{\sim} \mathrm{Div}(G)$$

with inverse map $[a] \mapsto (x \vee a)$.

This gives a complete description of the divisor group $\mathrm{Div}(G)$ and its relationship to the unit group of $\widetilde{G}(x)$, namely,

$$G(x) \cong G \times \mathbb{Z} \times G(x)^0.$$

5. Dequantization of Prüfer and Bézout domains

Proposition 3.1 suggests a study of abelian ℓ-groups via semi-domains. A first step of this program has already been taken in Section 3, where a decomposition of polynomials into linear factors has been achieved. Now let us come "back to the roots". The good news is that they are most easily calculated from the coefficients. For an abelian ℓ-group G and a polynomial $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \widetilde{G}[x]$ with $a_0a_n \neq 0$, it is not hard to show that all coefficients a_i can be assumed to be non-zero, that is, they belong to G. (This is of course not true for polynomials over a field, but note that in the tropical case, the zero element is the absolutely smallest one, smaller than every element of G.) By (Rump, 2015), Propositions 3 and 4, we have the following explicit formula for the roots: $d_i = b_{i-1}b_i^{-1}$, where

$$b_j := a_j \vee \bigvee_{i<j<k} (a_i^{k-j}a_k^{j-i})^{\frac{1}{k-i}}.$$

So the roots d_i of each polynomial are expressible in terms of k-th roots, where k does not exceed the degree of the polynomial f. Compared with the efforts of classical algebra up to the final stroke after Ruffini, Abel, and Galois - a quick victory!

However, as already mentioned, roots are not solutions. Nevertheless, the decomposition into linear factors indicates a close relationship to classical solutions. Indeed, here is a point where tropical algebra applies to the classical case.

Recall that a *fractional ideal* of an integral domain R with quotient field K is a non-zero R-submodule I of K such that $I \subset Ra$ for some $a \in K^\times$. A fractional ideal I is said to be *invertible* if there is a (necessarily unique) fractional ideal I^{-1} with $I^{-1}I = R$. Note that every invertible fractional ideal is finitely generated. An integral domain R is said to be a *Prüfer domain* (see (Gilmer, 1992), chap. IV) if the non-zero finitely generated ideals are invertible. If every non-zero finitely generated ideal of R is principal (hence invertible), R is called a *Bézout domain*.

The invertible fractional ideals of a Prüfer domain R form an abelian ℓ-group $G(R)$ with respect to inclusion. Note that

$$(I + J)(I \cap J) = IJ$$

holds for $I, J \in G(R)$, which shows that $G(R)$ is closed under finite intersection. In the special case that R is a Bézout domain, $(G(R); \supset)$ can be identified with $K^\times/R^\times$, the *group of divisibility* of R (see (Gilmer, 1992), section 16).

For a Prüfer domain R, the finitely generated ideals form a tropical semi-domain $A(R)^-$, the *dequantization* of R. By Proposition 3.2 and the Jaffard-Ohm correspondence (Jaffard, 1953; Ohm, 1966), every tropical semi-domain occurs as the dequantization of a Bézout domain. Thus, tropical algebra makes no difference between Prüfer domains and the more special Bézout domains. Since $A(R)^-$ is a semi-domain, we consider its quotient semifield $A(R)$, consisting of all finitely generated R-submodules of K. There is a natural map

$$t\colon K \to A(R) \tag{5.1}$$

from the quotient field K of R to $A(R)$, given by $t(a) := Ra$. Note that t is a monoid homomorphism, but not a morphism of semirings since $R(a + b)$ need not be equal to $Ra + Rb$.

This is by no means an anomaly. To the contrary, here is another point where tropical concepts enter the classical world. Recall that a *valuation* of a field K is a function $v\colon K \to \Gamma$ into a totally ordered abelian group Γ, augmented by an element ∞ with $\alpha + \infty = \infty$ for all $\alpha \in \Gamma \sqcup \{\infty\}$ such that the following are satisfied:

$$v(a) = \infty \iff a = 0 \tag{5.2}$$
$$v(ab) = v(a) + v(b) \tag{5.3}$$
$$v(a+b) \geqslant \min\{v(a), v(b)\}. \tag{5.4}$$

In a time where order-theoretic terms have been almost completely eliminated from the standard curriculum[1], such a function v which is not a morphism in any sense should sting in the eye! Let us rewrite (5.2)-(5.4) as follows. Endow Γ with the opposite order and write it multiplicatively. Then ∞ becomes 0 with $\alpha \cdot 0 = 0$ for all $\alpha \in \Gamma \sqcup \{0\}$, and the inequality (5.4) turns into

$$v(a+b) \leqslant v(a) \vee v(b).$$

So $\tilde{\Gamma} := \Gamma \sqcup \{0\}$ becomes a tropical semifield. The map (5.1) is characterized by the following universal property:

Proposition 5.1. *Let R be a Prüfer domain with quotient field K. Then every valuation $v\colon K \to \tilde{\Gamma}$ with $v(R) \leqslant 1$ factors uniquely through $t\colon K \to A(R)$*

$$\begin{tikzcd} K \arrow[r, "t"] \arrow[dr, "v"'] & A(R) \arrow[d, dotted, "f"] \\ & \tilde{\Gamma} \end{tikzcd} \tag{5.5}$$

such that $f\colon A(R) \to \tilde{\Gamma}$ is a morphism of semifields.

Proof. Define $f\colon A(R) \to \tilde{\Gamma}$ by $f(I) := \bigvee\{v(a) \mid a \in I\}$. Since every $I \in A(R)$ is of the form $I = Ra_1 + \cdots + Ra_n$, every $a = r_1a_1 + \cdots + r_na_n \in I$ with $r_i \in R$ satisfies $v(a) \leqslant v(a_1) \vee \cdots \vee v(a_n)$, which shows that f is well defined and renders (5.5) into a commutative diagram. The uniqueness of f is obvious. □

For an abelian ℓ-group G, the pure polynomial $1 \vee x^n$ is "purely inseparable":

$$1 \vee x^n = (1 \vee x)^n.$$

Therefore, the Frobenius identity

$$(a \vee b)^n = a^n \vee b^n$$

[1]It seems that Grothendieck's aversion against valuations had its bearing on this. In a letter of October 26, 1961, Serre complained: "You are very harsh on Valuations! I persist nonetheless in keeping them, for several reasons ...". Grothendieck's unrepentant response (October 31, 1961): "Your argument in favor of valuations is pretty funny ..."

holds in G, and (Darnel, 1995), 47.11, implies that G is a subdirect product of linearly ordered abelian groups. Thus, for a Prüfer domain R, the diagram (5.5) can be expressed by a single map

$$K^{\times} \xrightarrow{t} A(R)^{\times} \hookrightarrow \prod \Gamma,$$

where Γ runs through the value groups of all valuations of R. Moreover, t is surjective if and only if R is a Bézout domain. Examples of Bézout domains abound. The most prominent examples are the ring of algebraic integers ((Kaplansky, 1974), Theorem 102) and the ring of entire functions (Helmer, 1940). The ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials $f \in \mathbb{Q}[x]$ is an example of a Prüfer domain which is not a Bézout domain (Brizolis, 1979) (cf. (Narkiewicz, 1995), VII). In contrast to $\mathbb{Z}[x]$, which is not a Prüfer domain, $\mathrm{Int}(\mathbb{Z})$ has an uncountable number of maximal ideals, while both rings have Krull dimension 2.

The valuations $v\colon R \to \widetilde{\Gamma}$ or rather their extensions

$$v\colon K \to \widetilde{\Gamma}$$

to K are just the components of the tropicalization t. Thus, if V is a valuation domain with quotient field K, the corresponding valuation is just the tropicalization

$$t\colon K \to A(V),$$

and $A(V)^{\times}$ is the value group of V. There is a natural extension $t'\colon K[x] \to A(V)[x]$ via $t'(x) := x$. Explicitly:

$$t'(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = t(a_0) \vee t(a_1)x \vee t(a_2)x^2 \vee \cdots \vee t(a_n)x^n.$$

Note that $K[x]$ is even a principal ideal domain. We add a prime to make sure that t' cannot be confused with the restriction of $t\colon K(x) \to A(K[x])$ to $K[x]$.

For higher rank valuations, Hensel's lemma, which roughly states that coprime factorizations of polynomials modulo the maximal ideal can be lifted, is no longer valid (see (Engler & Prestel, 2005), Remark 2.4.6). What remains is that the topology of a field K with a complete valuation extends uniquely to fields L which are finite over K (Roquette, 1958). The proper substitute for complete valuation rings (where Hensel's lemma merely holds in rank 1) are the *Henselian* local rings, introduced by Azumaya (Azumaya, 1951) and developed by Nagata (Nagata, 1962), which satisfy Hensel's lemma by definition. For equivalent characterizations, see (Ribenboim, 1985). The most important characterization of Henselian local integral domains is that every integral extension is local ((Nagata, 1954), Theorem 7). For Henselian valuations of a field K, this means that they uniquely extend to the algebraic closure $\overline{K}$.

Proposition 5.2. *Let V be a Henselian valuation domain with quotient field K. Then $t\colon K \to A(V)$ extends uniquely to the algebraic closure $\overline{K}$ of K, which gives a commutative diagram*

$$\begin{tikzcd} K \arrow[r, "t"] \arrow[d, hook] & A(V) \arrow[d, hook] \\ \overline{K} \arrow[r, "t"] & A(V)^d. \end{tikzcd}$$

For every non-zero polynomial $f \in K[x]$ with roots $\alpha_1, \ldots, \alpha_n \in \overline{K}$, the roots of $t'(f)$ are $t(\alpha_1), \ldots, t(\alpha_n)$.

Proof. Since V is Henselian, the integral closure S of V in $\overline{K}$ is local, hence a valuation ring ((Bourbaki, 1972), VI.8.6, Proposition 6). Furthermore, $A(S)$ can be identified with the divisible closure of $A(V)$. If a is the leading coefficient of f, we have $f = a(x - \alpha_1) \cdots (x - \alpha_n)$ in $\overline{K}[x]$. Since t' is multiplicative, this implies that $t'(f) = t(a)(x \vee t(\alpha_1)) \cdots (x \vee t(\alpha_n))$. As $A(V)^d$ is linearly ordered, this proves the claim. □

Proposition 5.2 is the basis for Newton's method, which makes use of the following result. Its first part is essentially due to Ostrowski (Ostrowski, 1935).

Proposition 5.3. *Let V be a Henselian valuation domain with quotient field K, and let $f = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ be a non-zero polynomial. If f is irreducible, $t'(f)$ has a single root in $A(V)^d$. Conversely, if $t'(f)$ has a single root in $A(V)^d$, and there is no divisor $d > 1$ of n such that $A(V)^\times$ contains a d-th root of $t(a_0 a_n^{-1})$, then f is irreducible.*

Proof. Let S be the integral closure of V in the splitting field L of f. Every element σ of the Galois group $G(L|K)$ leaves S invariant: $\sigma(S) = S$. Hence, if f is irreducible, every zero α of f satisfies $t(\sigma(\alpha)) = t(\alpha)$ for all $\sigma \in G(L|K)$. So there is a single root $t(\alpha)$ of $t'(f)$ of multiplicity $\deg f$.

Conversely, assume that $t'(f)$ has a single root in $A(V)^d$, and that there is no divisor $d > 1$ of n such that $A(V)^\times$ contains a d-th root of $t(a_0 a_n^{-1})$. Let g be a monic irreducible factor of f. Without loss of generality, we can assume that $a_n = 1$. Then the single root α of $t'(f)$ satisfies $t'(f) = (x \vee \alpha)^n$ and $\alpha^n = t(a_0)$. If g is of degree m, then $t'(g) = (x \vee \alpha)^m$. Let $d > 0$ be the greatest common divisor of m and n. Then $d = pm + qn$ for some integers $p, q \in \mathbb{Z}$. Hence $h := (x \vee \alpha)^d = t'(g)^p t'(f)^q \in A(V)[x]$, and $d|m$ implies that $t'(g) = h^{m/d}$. Furthermore, the absolute term $a := \alpha^d$ of h belongs to $A(V)^\times$, and $a^{n/d} = t(a_0)$. By assumption, this gives $d = n$. Whence $f = g = h$ is irreducible. □

Proposition 5.3 reduces irreducibility of polynomials over K almost completely to the tropical semifield $A(V)$, where the complete factorization is obtained by straightforward calculation. Contrary to a remark in (Khanduja & Saha, 1997), the condition of the criterion is not necessary, as the trivial example $1 + x + x^2 \in \widehat{\mathbb{Q}}_2[x]$ shows. (The mistake is caused by rewriting the special version of Popescu and Zaharescu (Popescu & Zaharescu, 1995) in a logically different way.) In particular, we have the following

Corollary. *Let V be a Henselian valuation domain with quotient field K, and let $f = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ be a non-zero polynomial. If $t'(f)$ has m distinct roots, f splits into m relatively prime factors.*

Newton's method was applied already in the early days of valuation theory, invented by Hensel (Hensel, 1908), and developed by Kürschák (Kürschák, 1913*a*; Kürschák, 1913*b*), Ostrowski (Ostrowski, 1916, 1917, 1933), and Rychlík (Rump & Yang, 2008; Rychlík, 1924). Newton's method also appears in a paper of Rella (Rella, 1927), but in essence, it can even be traced back to Newton himself via Puiseux's theorem which states, in modern terms, that the field of Puiseux series over

$\overline{\mathbb{C}}$ is the algebraic closure of the field $\mathbb{C}((x))$ of formal Laurent polynomials, the quotient field of $\mathbb{C}[[x]]$.

Here the field $\mathbb{C}((x))$ not only builts a bridge between algebraic curves and complex analysis; in addition, it is maximally close to its tropical shadow: Every finite extension field of $\mathbb{C}((x))$ is isomorphic to $\mathbb{C}((x))$, the extension being just given be extracting some n-th root of x. So if S denotes the the integral closure S of $\mathbb{C}[[x]]$ in the algebraic closure of $\mathbb{C}((x))$, the tropical picture is encoded in the commutative diagram

$$\begin{tikzcd} \mathbb{C}((x)) \arrow[r, "t"] \arrow[d, hook] & A(\mathbb{C}[[x]]) = \mathbb{Z} \arrow[d, hook] \\ \overline{\mathbb{C}((x))} \arrow[r, "t"] & A(S) = \mathbb{Q}. \end{tikzcd}$$

A lot of irreducibility criteria can be derived from Proposition 5.3, which seems to be the "true metaphysics"[2] behind polynomial factorization. Eisenstein's criterion is just the first of a series of irreducibility criteria (e. g., (Dumas, 1906; Kürschák, 1923; Ore, 1923, 1924; Rella, 1927; MacLane, 1938; Azumaya, 1951)) which follow the same "tropical" pattern.

6. Algebraic equations in characteristic 1

Now we return to the problem that solutions of equations between tropical polynomials cannot just be read off from the roots. Let us start with linear equations

$$ax \vee b = cx \vee d \tag{6.1}$$

in a tropical semifield K. Looking quite innocent, they already bear a mild challenge. In contrast to classical algebra, such an equation is not always solvable. To avoid trivialities, assume that $a, b, c, d \in G := K^{\times}$. Then x cannot be zero, unless $b = d$. To solve Eq. (6.1), consider the map $p\colon G \to G$ given by

$$p(x) := \big((ad \vee bc)x \vee bd\big)\big(acx \vee (ad \vee bc)\big)^{-1}. \tag{6.2}$$

Note the expression $\Delta := ad \vee bc$ which looks like a determinant! The roots of the left- and right-hand side of Eq. (6.1) are respectively

$$\alpha := a^{-1}b, \qquad \beta := c^{-1}d.$$

Proposition 6.1. *The map (6.2) is idempotent and maps G onto the interval*

$$[\alpha \wedge \beta, \alpha \vee \beta]. \tag{6.3}$$

Every solution x of Eq. (6.1) is mapped into a solution $p(x)$.

[2]A common expression of the 18th century (see (Carnot, 1860); or (Speiser, 1956), Chapter 17, concerning Lagrange who considered groups as "la vraie métaphysique" of algebraic equations).

Proof. To verify that $p^2 = p$, note first that $\Delta^2 \geqslant abcd$. Now Eq. (6.2) can be written as

$$p(x) = \frac{\Delta x \vee bd}{acx \vee \Delta}.$$

So we have

$$p(p(x)) = \frac{\Delta(\Delta x \vee bd)(acx \vee \Delta)^{-1} \vee bd}{ac(\Delta x \vee bd)(acx \vee \Delta)^{-1} \vee \Delta} = \frac{\Delta(\Delta x \vee bd) \vee bd(acx \vee \Delta)}{ac(\Delta x \vee bd) \vee \Delta(acx \vee \Delta)}$$
$$= \frac{(\Delta^2 \vee abcd)x \vee \Delta bd}{ac\Delta x \vee (\Delta^2 \vee abcd)} = \frac{\Delta^2 x \vee \Delta bd}{ac\Delta x \vee \Delta^2} = \frac{\Delta x \vee bd}{acx \vee \Delta} = p(x).$$

Furthermore,

$$\begin{aligned} p(x) &= (\Delta x \vee bd)(acx \vee \Delta)^{-1} = (\Delta x \vee bd)(a^{-1}c^{-1}x^{-1} \wedge \Delta^{-1}) \\ &= \Delta x(a^{-1}c^{-1}x^{-1} \wedge \Delta^{-1}) \vee bd(a^{-1}c^{-1}x^{-1} \wedge \Delta^{-1}) \\ &\leqslant \Delta a^{-1}c^{-1} \vee bd\Delta^{-1} = a^{-1}b \vee c^{-1}d, \end{aligned}$$

and similarly, $p(x) = (\Delta x \vee bd)a^{-1}c^{-1}x^{-1} \wedge (\Delta x \vee bd)\Delta^{-1} \geqslant \Delta a^{-1}c^{-1} \wedge bd\Delta^{-1} = a^{-1}b \wedge c^{-1}d$. Thus p maps into the interval $[\alpha \wedge \beta, \alpha \vee \beta]$. For $x \in [\alpha \wedge \beta, \alpha \vee \beta]$, we have $acx \leqslant ac(a^{-1}b \vee c^{-1}d) = \Delta$, and secondly, $bd \leqslant (ad \vee bc)(a^{-1}b \wedge c^{-1}d) \leqslant \Delta x$. Hence $p(x) = (\Delta x \vee bd)\Delta^{-1} = \Delta x \Delta^{-1} = x$.

Finally, if x is a solution of Eq. (6.1), then $(ap(x) \vee b)(acx \vee \Delta) = a(\Delta x \vee bd) \vee b(acx \vee \Delta) = a\Delta x \vee b\Delta = (cx \vee d)\Delta = (c\Delta \vee acd)x \vee d(bc \vee \Delta) = c(\Delta x \vee bd) \vee d(acx \vee \Delta) = (cp(x) \vee d)(acx \vee \Delta)$, which shows that $p(x)$ is a solution of Eq. (6.1). □

By Proposition 6.1, the solutions of Eq. (6.1) are the fibers of the solutions in the interval (6.3) under the projection p. So it remains to consider solutions in the interval (6.3). To solve the equation, we consider another map $s\colon G \to G$ with

$$s(x) := a^{-1}d(ax \vee b)(cx \vee d)^{-1}. \tag{6.4}$$

Proposition 6.2. *The map (6.4) satisfies $s^2 = p$. In particular, s is an involution on the interval (6.3).*

Proof. We have

$$s(s(x)) = a^{-1}d \cdot \frac{a \cdot a^{-1}d(ax \vee b)(cx \vee d)^{-1} \vee b}{c \cdot a^{-1}d(ax \vee b)(cx \vee d)^{-1} \vee d} = a^{-1}d \cdot \frac{d(ax \vee b) \vee b(cx \vee d)}{ca^{-1}d(ax \vee b) \vee d(cx \vee d)}$$
$$= \frac{d(ax \vee b) \vee b(cx \vee d)}{c(ax \vee b) \vee a(cx \vee d)} = \frac{\Delta x \vee bd}{acx \vee \Delta} = p(x).$$ □

Corollary. *The following are equivalent.*

(a) *Eq. (6.1) is solvable.*
(b) *$ad \wedge bc \leqslant ab \leqslant ad \vee bc$.*

(c) $ad \wedge bc \leqslant cd \leqslant ad \vee bc$.

If Eq. (6.1) *is solvable, the unique solution in the interval* (6.3) *is* $x = (b \vee d)(a \vee c)^{-1}$.

Proof. The equivalence of (b) and (c) follows by symmetry. Condition (c) is equivalent to $a^{-1}d \in [\alpha \wedge \beta, \alpha \vee \beta]$. Furthermore, Eq. (6.4) shows that s maps every solution of Eq. (6.1) to $a^{-1}d$. Hence, if Eq. (6.1) is solvable, there is a solution $x \in [\alpha \wedge \beta, \alpha \vee \beta]$, which yields $a^{-1}d = s(x) = sp(x) = s^3(x) = ps(x) \in [\alpha \wedge \beta, \alpha \vee \beta]$. Thus (c) is necessary for the solvability of Eq. (6.1). Moreover, $x = p(x) = s^2(x) = s(a^{-1}d) = a^{-1}d(d \vee b)(ca^{-1}d \vee d)^{-1} = (d \vee b)(c \vee a)^{-1}$.

Conversely, if $a^{-1}d \in [\alpha \wedge \beta, \alpha \vee \beta]$, then $x := s(a^{-1}d)$ satisfies $s(x) = p(a^{-1}d) = a^{-1}d$. Hence Eq. (6.4) implies that x is a solution. $\square$

Our discussion of linear equations already shows that solutions need not exist, even for non-trivial equations. Therefore, a concept of algebraically closed semifield has to take this into account. So we arrive at the following

Definition 6.1. A semifield K is said to be *algebraically closed* if every equation $f(x) = 1$ with $f \in K(x)$ which is solvable in some extension semifield of K admits a solution in K.

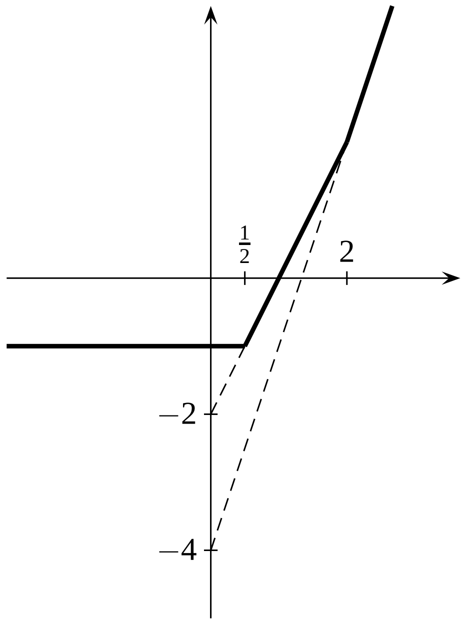
Note that an equation $f(x) = 1$ in $K(x)$ can also be written in the form

$$g(x) = h(x)$$

with polynomials $g, h \in K[x]$. We mention here that polynomials in $K[x]$ can be regarded as functions. Namely, for a non-trivial abelian ℓ-group G, Proposition 5 of (Rump, 2015) implies that $f \in \widetilde{G}[x]$ is uniquely determined by the corresponding function $f\colon G^d \to G^d$ on the divisible closure of G. For $\widetilde{G} = \mathbb{R}^+_{\max}$, it is convenient to write $\mathbb{R}^+$ additively via the logarithm. So G is turned into the additive group of $\mathbb{R}$, and 0 becomes $-\infty$. The graph of a polynomial is then piecewise linear, a classical Newton polygon. For example, the polynomial

$$-1 \vee (-2 + 2x) \vee (-4 + 3x)$$

looks as follows:



Here the coefficients are in $\mathbb{Z}$, while the roots are in $\frac{1}{2}\mathbb{Z}$, because the linear term is missing. The root $\frac{1}{2}$ is of multiplicity 2. Thus, if we add a linear term to get the polynomial into the normal form, the coefficient of x would be $-\frac{3}{2}$.

The corollary of Proposition 6.2 shows that in the tropical case, linear equations are not trivial, and that roots only play a certain rôle with respect to the solutions. In compensation for this initial difficulty of tropical equations, Theorem 4 of (Rump, 2015) states that we don't have to go beyond quadratic equations! Precisely, the theorem says that a tropical semifield K is algebraically closed if and only if the ℓ-group $G := K^\times$ is divisible, that is, the pure equations $x^n = a$ are solvable in G, and the quadratic equations

$$(a \vee 1)x^2 \vee (a^2 \vee b \vee 1)x \vee (a^2 \vee a) = ax^2 \vee a \tag{6.5}$$

are solvable for all $a, b \in G$. Note that the solvablity clause (in an extension semifield) of Definition 6.1 is missing. In fact, we have

Proposition 6.3. *The equations* (6.5) *are solvable in any totally ordered abelian group.*

Proof. For $a \geqslant 1$, Eq. (6.5) becomes $ax^2 \vee (a^2 \vee b)x \vee a^2 = ax^2 \vee a$. We show that this equation holds for all $x \geqslant a \vee a^{-1}b$. Indeed, the latter implies that $ax^2 \geqslant ax(a \vee a^{-1}b) = (a^2 \vee b)x \geqslant a^2$. So the equation (6.5) is solved. For $a \leqslant 1$, the equation becomes $x^2 \vee (b \vee 1)x \vee a = ax^2 \vee a$. Here we choose $x \leqslant a(b \vee 1)^{-1}$. Then $x \leqslant a$ and $(b \vee 1)x \leqslant a$. Hence $ax^2 \leqslant x \leqslant a$, which solves the equation. □

Corollary 1. *For any tropical semifield, there exists a (tropical) extension semifield where Eq.* (6.5) *is solvable.*

Proof. This follows since every abelian ℓ-group G is a subdirect product of totally ordered abelian groups ((Darnel, 1995), 47.11). □

Furthermore, Theorem 4 of (Rump, 2015) implies

Corollary 2. *Let G be a totally ordered abelian group. Then $\widetilde{G}$ is algebraically closed if and only if the pure equation $x^n = a$ is solvable for all positive integers n and $a \in G$.*

To analyse Eq. (6.5), consider an additive abelian ℓ-group G. The proof of Proposition 6.3 then tells us that in the totally ordered case, solutions of Eq. (6.5) exist, but depending on the sign of a, they must be either large enough if $a > 0$ or small enough if $a < 0$.

It is this point where geometry enters the scene. By the Jaffard-Ohm correspondence, every abelian ℓ-group G occurs as a tropicalized Bézout domain R. By (**?**), Proposition 7, the structure sheaf of R can be transferred to G, which yields a sheaf $\breve{G}$ on a spectral space X with totally ordered stalks such that $\Gamma(X, \breve{G}) \cong G$. In the archimedean case, $\breve{G}$ is a sheaf of germs of continuous functions. Therefore, the sensitivity of Eq. (6.5) against sign change of a is best illustrated by the following

Example. Let G be the ℓ-group $\mathscr{C}[-1,1]$ of continuous real functions on the closed interval $[-1,1]$. Multiplying Eq. (6.5) by $a^{-1}x^{-1}$, it takes the symmetric form

$$a^{-}x \vee c \vee a^{+}x^{-1} = |x| \tag{6.6}$$

with $a \in G$ and $c \geqslant |a|$, where $|a| := a \vee a^{-1}$ and

$$a^{+} := a \vee 1, \qquad a^{-} := a^{-1} \vee 1.$$

Writing Eq. (6.6) additively, it becomes

$$(a^{-} + x) \vee c \vee (a^{+} - x) = |x|.$$

Passing to $\mathscr{C}[-1,1]$, let c be the constant function $t \mapsto 1$, and let a be arbitrary with $|a| \leqslant c$. If $x(t) \geqslant 0$, this implies that $x(t) = |x|(t) \geqslant 1$, while $x(t) \leqslant 0$ gives $-x(t) \geqslant 1$, that is, $x(t) \leqslant -1$. Thus Eq. (6.5) cannot be solvable by a continuous function.

Recall that an element $u \geqslant 1$ of a (multiplicative) abelian ℓ-group G is said to be a *weak order unit* ((Darnel, 1995), 54.3) if $u \wedge a = 1$ implies that $a = 1$. For $a \in G^{+}$, we write $G(a)$ for the ℓ-ideal generated by a. It consists of the elements $x \in G$ with $|x| \leqslant a^n$ for some $n \in \mathbb{N}$.

Definition 6.2. (McGovern, 2005) An abelian ℓ-group G is said to be *weakly complemented* if for any pair $a, b \in G$ with $a \wedge b = 1$, there exist $a', b' \in G$ with $a \leqslant a'$ and $b \leqslant b'$ such that $a' \wedge b' = 1$ and $a'b'$ is a weak order unit of G. If $G(a)$ is weakly complemented for all $a \in G^{+}$, then G is called *locally weakly complemented*.

The following result shows that the solvability of Eq. (6.5) merely depends on the lattice structure of G. To state it, we need a very weak form of projectability. Recall that an abelian ℓ-group G is *strongly projectable* (Darnel, 1995) if the *polar*

$$I^{\perp} := \{a \in G \mid \forall\, b \in I \colon |a| \wedge |b| = 1\}$$

of any ℓ-ideal I is a cardinal summand: $G = I^{\perp} \boxplus I^{\perp\perp}$. If this holds for principal ℓ-ideals $I = G(a)$, then G is called *projectable*. More generally, G is said to be *semi-projectable*[3] (Bigard *et al.*, 1977) if

$$(a \wedge b)^{\perp} = a^{\perp} b^{\perp}$$

for $a, b \in G^{+}$. (For a geometric characterization, see (Rump, 2014), corollary of Theorem 1.) Still more generally, we call G *z-projectable* (Rump, 2014) if

$$(ab)^{\perp\perp} = a^{\perp\perp} b^{\perp\perp}$$

holds for $a, b \in G^{+}$. Thus

$$\boxed{\text{strongly projectable} \implies \text{projectable} \implies \text{semi-projectable} \implies z\text{-projectable}}$$

All these concepts are pairwise inequivalent. The line of implications could even be enlarged to seven types of projectability (Rump, 2014) which all have their particular relevance (cf. the hierarchy of T_n-spaces in general topology). Now we are ready to prove

Theorem 6.1. *Let G be an abelian ℓ-group. The following are equivalent.*

(a) *The quadratic equations (6.5) are solvable in G.*
(b) *For $a, b, c \in G$ with $a \wedge b = 1$ and $c \geqslant a \vee b$, there exist $a', b' \in G$ with $a' \geqslant a$ and $b' \geqslant b$ such that $a' \wedge b' = 1$ and $a' \vee b' = c$.*
(c) *G is semi-projectable and locally weakly complemented.*
(d) *G is z-projectable and locally weakly complemented.*

Proof. (a) $\Rightarrow$ (b): By assumption, there exists a solution $x \in G$ of Eq. (6.6) with ab^{-1} instead of a. Then $bx \leqslant x^{+}x^{-}$ and $ax^{-1} \leqslant x^{+}x^{-}$, which gives $(x^{-})^2 \geqslant b$ and $(x^{+})^2 \geqslant a$. Define $a' := (x^{+})^2 \wedge c$ and $b' := (x^{-})^2 \wedge c$. Then $a' \wedge b' = 1$ and $a' \vee b' = \big((x^{+})^2 \vee (x^{-})^2\big) \wedge c = c$.

(b) $\Rightarrow$ (c): Let $P \neq Q$ be minimal prime ℓ-ideals of G. Choose $a \in P \cap G^{+} \setminus Q$. Since P is minimal, $a \wedge b = 1$ for some $b \notin P$. For any $c \geqslant a \vee b$, the elements a', b' in (b) satisfy $a' \in b^{\perp}$ and $b' \in a^{\perp}$. Hence $a^{\perp} b^{\perp} = G$. Since $a^{\perp} \subset Q$ and $b^{\perp} \subset P$, we obtain $PQ = G$, which shows that G has stranded primes. By (Bigard *et al.*, 1977), Proposition 7.5.1, this implies that G is semi-projectable. Moreover, (b) implies that G is locally weakly complemented.

(c) $\Rightarrow$ (d): By (Rump, 2014), Proposition 4, every semi-projectable abelian ℓ-group is z-projectable.

(d) $\Rightarrow$ (a): Let $a, b, c \in G$ with $a \wedge b = 1$ and $c \geqslant a \vee b$ be given. By the equivalence of Eq. (6.5) and Eq. (6.6), it is enough to solve the equation

$$ax \vee c \vee bx^{-1} = |x|. \tag{6.7}$$

[3] Some authors replace this term by "having stranded primes", referring to an equivalent form proved in (Bigard *et al.*, 1977), Proposition 7.5.1. Darnel (Darnel, 1995) argues that "semi-projectable" does not come close to "projectable" (referring perhaps to the "projections" of a cardinal sum). Note, however, the equivalent version $a \wedge b = 1 \Rightarrow a^{\perp} b^{\perp} = G$, which gives half of a cardinal sum: "semi" $\times$ "projectable".

By assumption, there exist $a', b' \in G$ with $a' \geqslant a$ and $b' \geqslant b$ such that $a' \wedge b' = 1$ and $(a'b')^{\perp} \cap G(c) = \{1\}$. Since G is z-projectable, this yields $c \in (a'b')^{\perp\perp} = (a')^{\perp\perp}(b')^{\perp\perp}$. So there are $p \in (a')^{\perp\perp} \cap G^{+}$ and $q \in (b')^{\perp\perp} \cap G^{+}$ with $c = pq$. In particular, this implies that $p \wedge q = 1$. Hence $a = a \wedge (p \vee q) = (a \wedge p) \vee (a \wedge q) = a \wedge p$. So we have $a \leqslant p$, and similarly, $b \leqslant q$. Thus $x := qp^{-1}$ solves Eq. (6.7). □

By (Rump, 2015), Theorem 4, we obtain

Corollary 1. *Let G be an abelian ℓ-group. The tropical semifield $\widetilde{G}$ is algebraically closed if and only if G is divisible and its underlying lattice satisfies condition (b) of Theorem 6.1.*

Recall that a ring R is said to be *clean* (Nicholson, 1977) if every $a \in R$ is a sum of an idempotent and a unit. Nicholson (Nicholson, 1977) proved that a clean ring R satisfies the *exchange property* (Crawley & Jónsson, 1964; Warfield, 1972), which means that for every decomposition $M = R \oplus N = \bigoplus_{i \in I} M_i$ of modules, there are submodules $M_i' \subset M_i$ with $M = R \oplus \bigoplus_{i \in I} M_i'$. For example, commutative von Neumann regular rings, and semiperfect rings, are clean. For various characterizations, see (McGovern, 2005). If every non-isomorphic homomorphic image of R is clean, the ring R is called *neat* (McGovern, 2005).

Corollary 2. *A Bézout domain is neat if and only if its group of divisibility satisfies the equivalent conditions of Theorem 6.1.*

Proof. By (McGovern, 2005), Theorem 5.7, a Bézout domain is neat if and only if its group of divisibility is semi-projectable and locally weakly complemented. Thus Theorem 6.1 applies. □

Remark. Note that the underlying lattice of an abelian ℓ-group is self-dual via $x \mapsto x^{-1}$. Thus, for a Bézout domain R, Corollary 2 remains valid if the group of divisibility is replaced by the unit group $A(R)^{\times}$ of the tropical semifield $A(R)$. In particular, Corollary 2 gives a characterization of Bézout domains R with $A(R)$ algebraically closed.

Finally, we consider the abelian ℓ-group $\mathscr{C}(X)$ of continuous real valued functions on a topological space X. Note that $\mathscr{C}(X)$ is also a ring. To avoid confusion, let us denote this ring by $C(X)$. By (Gillman & Jerison, 1960), Theorem 3.9, there is no loss of generality if X is assumed to be completely regular. It is known that $C(X)$ is a Bézout ring (that is, every finitely generated ideal is principal) if and only if X is an *F-space*, which originally was just defined by this property (Gillman & Henriksen, 1956). For equivalent characterizations, see (Gillman & Jerison, 1960), Theorem 14.25. One of these characterizations states that for every $f \in C(X)$ there is an element $g \in C(X)$ with $f = g|f|$.

Corollary 3. *Let X be a completely regular space. If the tropical semifield $\widetilde{\mathscr{C}(X)}$ is algebraically closed, then X is an F-space.*

Proof. Let $f \in C(X)$ be given. Then $(f^{+} \wedge 1) \wedge (f^{-} \wedge 1) = 0$ and $(f^{+} \wedge 1) \vee (f^{-} \wedge 1) \leqslant 1$. Thus, by Corollary 1, there exist $g, h \in \mathscr{C}(X)$ with $f^{+} \wedge 1 \leqslant g$ and $f^{-} \wedge 1 \leqslant h$ such that $g \wedge h = 0$ and $g \vee h = 1$. We claim that $f = (g - h)|f|$. If $f(t) > 0$, then $0 < f^{+}(t) \wedge 1 \leqslant g(t)$. Hence $h(t) = 0$, and thus $(g - h)(t) = 1$. Similarly, $f(t) < 0$ implies that $0 < f^{-}(t) \wedge 1 \leqslant h(t)$, which yields $(g - h)(t) = -1$. Thus X is an F-space. □

References

Anderson, M. and T. Feil (1988). *Lattice-ordered groups*. D. Reidel Publishing Co., Dordrecht.

Azumaya, G. (1951). On maximally central algebras. *Nagoya Math. J.* **2**, 119–150.

Bigard, A., K. Keimel and S. Wolfenstein (1977). *Groupes et anneaux réticulés, Lecture Notes in Mathematics*. Vol. 608, Springer-Verlag, Berlin-New York.

Birkhoff, G. (1942). Lattice ordered groups. *Ann. of Math.* **43**, 298–331.

Blok, W. J. and I. M. A. Ferreirim (2000). On the structure of hoops. *Algebra Univ.* **43**(2-3), 233–257.

Bohr, N. (1920). Über die serienspektra der elemente. *Zeitschrift f.Physik* **2**, 423–478.

Bourbaki, N. (1972). *Commutative algebra*. Hermann, Paris.

Brizolis, D. (1979). A theorem on ideals in pprüfer rings of integral-valued polynomials. *Comm. Algebra* **7**(10), 1065–1077.

Carnot, L. (1860). *Réflexions sur la métaphysique du calcul infinitésimal*. 4^{me} édition, Paris.

Castella, D. (2010). éléments d'algèbre linéaire tropicale. *Linear Algebra Appl.* **432**(6), 1460–1474.

Connes, A. and C. Consani (2010). Schemes over f_1 and zeta functions. *Compos. Math.* **146**(6), 1383–1415.

Connes, A. and C. Consani (2011). *Characteristic 1, entropy and the absolute point, Noncommutative geometry, arithmetic, and related topics*. Johns Hopkins Univ. Press, Baltimore, MD,.

Crawley, P. and B. Jónsson (1964). Refinements for infinite direct decompositions of algebraic systems. *Pacific J. Math.* **14**, 797–855.

Cuninghame-Green, R. A. and P. F. J. Meijer (1980). An algebra for piecewise-linear minimax problems. *Discrete Appl. Math.* **2**(4), 267–294.

Darnel, M. R. (1995). *Theory of lattice-ordered groups*. Monographs and Textbooks in Pure and Applied Mathematics, Marcel Dekker, Inc., New York.

Deitmar, A. (2008). f_1-schemes and toric varieties. *Beiträge Algebra Geom.* **49**(2), 517–525.

Dumas, G. (1906). Sur quelques cas d'irreductibilité des polynomes à coefficients rationnels. *Journal de Mathematique* **2**, 191–258.

Engler, A. J. and A. Prestel (2005). *Valued fields*. Springer Monographs in Mathematics, Springer-Verlag, Berlin.

Euler, L. (1911). *Vollständige Anleitung zur Algebra*. Teubner-Verlag, Berlin.

Gillman, L. and M. Henriksen (1956). Rings of continuous functions in which every finitely generated ideal is principal. *Trans. Amer. Math. Soc.* **82**, 366–391.

Gillman, L. and M. Jerison (1960). *Rings of continuous functions*. The University Series in Higher Mathematics D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto-London-New York.

Gilmer, R. (1992). *Multiplicative ideal theory, Corrected reprint of the 1972 edition*. Queen's Papers in Pure and Applied Mathematics, 90. Queen's University, Kingston, ON.

Glass, A. M. W. (1999). *Partially ordered groups*. Series in Algebra, 7, World Scientific Publishing Co., Inc., River Edge, NJ.

Greuel, G.-M. and H. Knörrer (1985). Einfache kurvensingularitäten und torsionsfreie moduln. *Math. Ann.* **270**(3), 417–425.

Helmer, O. (1940). Divisibility properties of integral functions. *Duke Math. J.* **6**, 345–356.

Hensel, K. (1908). *Theorie der Algebraischen Zahlen*. Leipzig.

Iséki, K. and S. Tanaka (1978). An introduction to the theory of bck-algebras. *Math. Japon.* **23**, 1–26.

Jaffard, P. (1953). Contribution à l'étude des groupes ordonnés. *J. Math. Pure Appl.* **32**, 203–280.

Kaplansky, I. (1974). *Commutative rings*. Revised ed., The University of Chicago Press, Chicago, Ill.-London.

Khanduja, S. K. and J. Saha (1997). On a generalization of Eisenstein's irreducibility criterion. *Mathematika* **44**(1), 37–41.

Kürschák, J. (1913*a*). Über limesbildung und allgemeine körpertheorie. *Proc. 5th Internat. Congress of Mathematicians, Cambridge* **1**, 285–289.

Kürschák, J. (1913*b*). Über limesbildung und allgemeine körpertheorie. *J. Reine Angew. Math.* **142**, 211–253.

Kürschák, J. (1923). Irreduzible formen. *Journal für die Mathematik* **152**, 180–191.

Lang, S. (1965). *Algebra*. Addison-Wesley Publishing Co., Inc., Reading,Mass.

Lescot, P. (2009). Algèbre absolue. *Ann. Sci. Math. Québec* **33**(1), 63–82.

Litvinov, G. L. (2006). The maslov dequantization, idempotent and tropical mathematics: a very brief introduction, idempotent mathematics and mathematical physics. *Amer. Math. Soc., Providence,RI*.

MacLane, S. (1938). The Schönemann-Eisenstein irreducibility criteria in terms of prime ideals. *Trans. Amer. Math. Soc.*

McGovern, W. Wm. (2005). Neat rings. *J. Pure Appl. Algebra* **377**, 1–17.

Nagata, M. (1954). On the theory of Henselian rings ii. *Nagoya Math. J.* **7**, 1–19.

Nagata, M. (1962). *Local rings*. John Wiley & Sons, New York, London.

Narkiewicz, W. (1995). *Polynomial mappings*. Springer LNM 1600, Berlin.

Nicholson, W. K. (1977). Lifting idempotents and exchange rings. *Trans. Amer. Math. Soc.* **229**, 269–278.

Ohm, J. (1966). Some counterexamples related to integral closure of $d[[x]]$. *Trans. Amer. Math. Soc.* **122**, 321–333.

Ore, Ö. (1923). Zur theorie der irreduzibilitätskriterien. *Math. Z.* **18**(1), 278–288.

Ore, Ö. (1924). Zur theorie der Eisensteinschen Gleichungen. *Math.Z.* **20**(1), 267–279.

Ostrowski, A. (1916). Über einige lösungen der funktionalgleichung $\psi(x)\cdot\psi(y) = \psi(xy)$. *Acta Math.* **41**(1), 271–284.

Ostrowski, A. (1917). Über sogenannte perfekte körper. *J. Reine Angew.Math.* **147**, 191–204.

Ostrowski, A. (1933). Über algebraische funktionen von dirichletschen reihen. *Math.Z.* **37**, 98–133.

Ostrowski, A. (1935). Untersuchungen zur arithmetischen theorie der körper. *Math.Z.* **39**, 269–404.

Popescu, N. and A. Zaharescu (1995). On the structure of the irreducible polynomials over local fields. *J. Number Theory* **52**(1), 98–118.

Rella, T. (1927). Ordnungsbestimmungen in integritätsbereichen und newtonsche polygone. *J. Reine Angew. Math.* **158**, 33–48.

Ribenboim, P. (1985). Equivalent forms of Hensel's lemma. *Exposition. Math.*

Riesz, F. (1910). Untersuchungen über systeme integrierbarer funktionen. *Math. Ann.* **69**, 449–497.

Roquette, P. (1958). On the prolongation of valuations. *Trans. Amer. Math. Soc.* **88**, 42–56.

Rump, W. (2008). *l*-algebras, self-similarity, and *l*-groups. *J. Algebra* **320**(6), 2328–2348.

Rump, W. (2014). Abelian lattice-ordered groups and a characterization of the maximal spectrum of a prüfer domain. *J. Pure Appl. Algebra* **218**(12), 2204–2217.

Rump, W. (2015). Algebraically closed abelian *l*-groups. *Math. Slovaca* **65**(4), 841–862.

Rump, W. and Y. C. Yang (2008). Jaffard-Ohm correspondence and Hochster duality.. *Bull. Lond. Math. Soc.* **40**(2), 263–273.

Rychlík, K. (1924). Zur bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153**, 94–107.

Simon, I. (1987). *Caracterização de conjuntos racionais limitados*. Tese de Livre-Docência, Instituto de Matemática e Estatística da Universidade de São Paulo.

Soulé, C. (2011). Lectures on algebraic varieties over f_1, noncommutative geometry, arithmetic, and related topics. *Johns Hopkins Univ. Press, Baltimore, M* pp. 267–277.

Speiser, A. (1956). *Die Theorie der Gruppen von endlicher Ordnung*. Birkhäuser Verlag, Basel und Stuttgart.

Warfield, R. B. (1972). Exchange rings and decompositions of modules. *Math. Ann.* **199**, 31–36.

Weil, A. (1940). Sur les fonctions algébriques à corps de constantes fini. *C. R. Acad. Sci. Paris* **210**, 592–594.

Weil, A. (1941). On the Riemann hypothesis in function fields. *Proc. Nat. Acad. Sci.* **27**, 345–347.

Weinert, J. J. and R. Wiegandt (1940). On the structure of semifields and lattice-ordered groups. *Period. Math. Hungar.* **32**(1), 129–147.