FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 63–72, 2017
DOI: 10.1515/forma-2017-0006

DE GRUYTER OPEN
degruyter.com/view/j/forma

Ordered Rings and Fields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. We introduce ordered rings and fields following Artin-Schreier's approach using positive cones. We show that such orderings coincide with total order relations and give examples of ordered (and non ordered) rings and fields. In particular we show that polynomial rings can be ordered in (at least) two different ways [8, 5, 4, 9]. This is the continuation of the development of algebraic hierarchy in Mizar [2, 3].

MSC: 12J15 03B35

Keywords: commutative algebra; ordered fields; positive cones

MML identifier: `REALALG1`, version: `8.1.05 5.40.1289`

1. On Order Relations

Let X be a set and R be a binary relation on X. We say that R is strongly reflexive if and only if

(Def. 1) R is reflexive in X.

We say that R is totally connected if and only if

(Def. 2) R is strongly connected in X.

One can check that there exists a binary relation on X which is strongly reflexive and there exists a binary relation on X which is totally connected and every binary relation on X which is strongly reflexive is also reflexive and every binary relation on X which is totally connected is also strongly connected.

Let X be a non empty set. One can check that every binary relation on X which is strongly reflexive is also non empty and every binary relation on X which is totally connected is also non empty.

Now we state the propositions:

ISSN 1426–2630(Print), 1898-9934(Online)

(1) Let us consider a non empty set X, a strongly reflexive binary relation R on X, and an element x of X. Then $x \leqslant_R x$.

(2) Let us consider a non empty set X, an antisymmetric binary relation R on X, and elements x, y of X. If $x \leqslant_R y$ and $y \leqslant_R x$, then $x = y$.

(3) Let us consider a non empty set X, a transitive binary relation R on X, and elements x, y, z of X. If $x \leqslant_R y$ and $y \leqslant_R z$, then $x \leqslant_R z$.

(4) Let us consider a non empty set X, a totally connected binary relation R on X, and elements x, y of X. Then

(i) $x \leqslant_R y$, or

(ii) $y \leqslant_R x$.

Let L be an additive loop structure and R be a binary relation on L. We say that R is respecting addition if and only if

(Def. 3) for every elements a, b, c of L such that $a \leqslant_R b$ holds $a + c \leqslant_R b + c$.

Let L be a multiplicative loop with zero structure. We say that R is respecting multiplication if and only if

(Def. 4) for every elements a, b, c of L such that $a \leqslant_R b$ and $0_L \leqslant_R c$ holds $a \cdot c \leqslant_R b \cdot c$.

2. On Minimal Non Zero Indices of Polynomials

Now we state the proposition:

(5) Let us consider a degenerated ring R, and a polynomial p over R. Then $\{i$, where i is a natural number : $p(i) \neq 0_R\} = \emptyset$.

Let us consider a ring R and a polynomial p over R.

(6) $p = \mathbf{0}.R$ if and only if $\{i$, where i is a natural number : $p(i) \neq 0_R\} = \emptyset$.

(7) $\min^*\{i$, where i is a natural number : $(p+\mathbf{0}.R)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$. The theorem is a consequence of (6).

(8) Let us consider a non degenerated ring R, and a polynomial p over R. Then $\min^*\{i$, where i is a natural number : $(-p)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$.

Let us consider a non degenerated ring R and non zero polynomials p, q over R. Now we state the propositions:

(9) Suppose $\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} > \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. Then $\min^*\{i$, where i is a natural number : $(p + q)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$.

(10) Suppose $p + q \neq \mathbf{0}.R$ and $\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. Then $\min^*\{i$, where i is a natural number : $(p+q)(i) \neq 0_R\} \geqslant \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$. The theorem is a consequence of (6).

(11) Suppose $p(\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}) + q(\min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}) \neq 0_R$. Then $\min^*\{i$, where i is a natural number : $(p + q)(i) \neq 0_R\} = \min(\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}, \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\})$. The theorem is a consequence of (9), (6), and (10).

(12) Suppose $p * q \neq \mathbf{0}.R$. Then $\min^*\{i$, where i is a natural number : $(p * q)(i) \neq 0_R\} \geqslant \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} + \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$.

(13) Let us consider an integral domain R, and non zero polynomials p, q over R. Then $\min^*\{i$, where i is a natural number : $(p * q)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} + \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. The theorem is a consequence of (12).

3. PRELIMINARIES

Let L be a non empty multiplicative loop structure and S be a subset of L. We say that S is closed under multiplication if and only if

(Def. 5) for every elements s_1, s_2 of L such that s_1, $s_2 \in S$ holds $s_1 \cdot s_2 \in S$.

Let L be a non empty additive loop structure. The functor $-S$ yielding a subset of L is defined by the term

(Def. 6) $\{-s$, where s is an element of $L : s \in S\}$.

Let L be an add-associative, right zeroed, right complementable, non empty additive loop structure. One can check that $--S$ reduces to S.

Now we state the proposition:

(14) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, a subset S of L, and an element a of L. Then $a \in S$ if and only if $-a \in -S$.

Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L and subsets S_1, S_2 of L. Now we state the propositions:

(15) $-S_1 \cap S_2 = (-S_1) \cap (-S_2)$.

(16) $-(S_1 \cup S_2) = -S_1 \cup -S_2$.

Let L be a non empty additive loop structure and S be a subset of L. We say that S is negative-disjoint if and only if

(Def. 7) $S \cap (-S) = \{0_L\}$.

We say that S is spanning if and only if

(Def. 8) $S \cup -S =$ the carrier of L.

4. Squares and Sums of Squares

Let us note that 0_R is a square and 1_R is a square and there exists an element of R which is a square.

Let a be an element of R. We say that a is a sum of squares if and only if

(Def. 9) there exists a finite sequence f of elements of R such that $\sum f = a$ and for every natural number i such that $i \in \operatorname{dom} f$ there exists an element a of R such that $f(i) = a^{\mathbf{2}}$.

Let us note that every element of R which is a square is also a sum of squares.

Let R be a commutative ring and a, b be square elements of R. Observe that $a \cdot b$ is a square. Let R be a ring and a, b be sum of squares elements of R. One can verify that $a + b$ is a sum of squares.

Let R be a commutative ring. Let us observe that $a \cdot b$ is a sum of squares.

Let R be a ring. The functors: Squares(R) and QuadraticSums(R) yielding subsets of R are defined by terms

(Def. 10) $\{a$, where a is an element of $R : a$ is a square$\}$,

(Def. 11) $\{a$, where a is an element of $R : a$ is a sum of squares$\}$,

respectively. We introduce the notation $\mathrm{SQ}(R)$ as a synonym of Squares(R) and $\mathrm{QS}(R)$ as a synonym of QuadraticSums(R).

One can check that $\mathrm{SQ}(R)$ is non empty and $\mathrm{QS}(R)$ is non empty.

Let S be a subset of R. We say that S has all squares if and only if

(Def. 12) $\mathrm{SQ}(R) \subseteq S$.

We say that S has all sums of squares if and only if

(Def. 13) $\mathrm{QS}(R) \subseteq S$.

One can check that there exists a subset of R which has all squares and there exists a subset of R which has all sums of squares and every subset of R which has all squares is also non empty and every subset of R which has all sums of squares is also non empty and every subset of R which has all sums of squares has also all squares and every subset of R which is closed under addition and has all squares has also all sums of squares and $\mathrm{SQ}(R)$ has all squares and $\mathrm{QS}(R)$ has all sums of squares.

Let us consider a ring R. Now we state the propositions:

(17) 0_R, $1_R \in \mathrm{SQ}(R)$.

(18) $\mathrm{SQ}(R) \subseteq \mathrm{QS}(R)$.

Let R be a ring. Note that $\mathrm{QS}(R)$ is closed under addition.

Let R be a commutative ring. Note that $\mathrm{QS}(R)$ is closed under multiplication.

Let us consider a ring R and a subring S of R. Now we state the propositions:

(19) $\mathrm{SQ}(S) \subseteq \mathrm{SQ}(R)$.

(20) $\mathrm{QS}(S) \subseteq \mathrm{QS}(R)$.

5. Positive Cones and Orderings

Let R be a ring and S be a subset of R. We say that S is a prepositive cone if and only if

(Def. 14) $S + S \subseteq S$ and $S \cdot S \subseteq S$ and $S \cap (-S) = \{0_R\}$ and $\mathrm{SQ}(R) \subseteq S$.

We say that S is a positive cone if and only if

(Def. 15) $S + S \subseteq S$ and $S \cdot S \subseteq S$ and $S \cap (-S) = \{0_R\}$ and $S \cup -S =$ the carrier of R.

One can check that every subset of R which is a prepositive cone is also non empty and every subset of R which is a positive cone is also non empty and every subset of R which is a prepositive cone is also closed under addition, closed under multiplication, and negative-disjoint and has also all squares.

Every subset of R which is closed under addition, closed under multiplication, and negative-disjoint and has all squares is also a prepositive cone and every subset of R which is a positive cone is also closed under addition, closed under multiplication, negative-disjoint, and spanning and every subset of R which is closed under addition, closed under multiplication, negative-disjoint, and spanning is also a positive cone and every subset of R which is a positive cone is also a prepositive cone.

Let us consider a field F and a subset S of F. Now we state the propositions:

(21) If $S \cdot S \subseteq S$ and $\mathrm{SQ}(F) \subseteq S$, then $S \cap (-S) = \{0_F\}$ iff $-1_F \notin S$.

(22) Suppose $S \cdot S \subseteq S$ and $S \cup -S =$ the carrier of F. Then $S \cap (-S) = \{0_F\}$ if and only if $-1_F \notin S$.

PROOF: $\mathrm{SQ}(F) \subseteq S$ by [7, (10)]. □

Let R be a ring. We say that R is preordered if and only if

(Def. 16) there exists a subset P of R such that P is a prepositive cone.

We say that R is ordered if and only if

(Def. 17) there exists a subset P of R such that P is a positive cone.

Let us note that there exists a field which is preordered and there exists a field which is ordered and every ring which is ordered is also preordered.

Let R be a preordered ring. One can verify that there exists a subset of R which is a prepositive cone.

Let R be an ordered ring. Let us note that there exists a subset of R which is a positive cone.

Let R be a preordered ring.

A preordering of R is prepositive cone subset of R.

Let R be an ordered ring.

An ordering of R is positive cone subset of R. Now we state the proposition:

(23) Let us consider a preordered ring R, a preordering P of R, and an element a of R. Then $a^{\mathbf{2}} \in P$.

Let us consider a preordered ring R and a preordering P of R. Now we state the propositions:

(24) $\mathrm{QS}(R) \subseteq P$.

(25) 0_R, $1_R \in P$. The theorem is a consequence of (24).

(26) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then $-1_R \notin P$. The theorem is a consequence of (25).

(27) Let us consider a preordered field F, a preordering P of F, and a non zero element a of F. If $a \in P$, then $a^{-1} \in P$. The theorem is a consequence of (23).

(28) Let us consider a preordered, non degenerated ring R. Then $\mathrm{char}(R) = 0$. The theorem is a consequence of (25) and (24).

(29) Let us consider an ordered ring R, and orderings O, P of R. If $O \subseteq P$, then $O = P$. The theorem is a consequence of (25).

6. Orderings vs. Order Relations

Let R be a preordered ring, P be a preordering of R, and a, b be elements of R. We say that $a \leqslant_b P$ if and only if

(Def. 18) $b - a \in P$.

The functor $\mathrm{OrdRel}\, P$ yielding a binary relation on R is defined by the term

(Def. 19) $\{\langle a, b\rangle$, where a, b are elements of $R : a \leqslant_b P\}$.

One can verify that $\mathrm{OrdRel}\, P$ is non empty and $\mathrm{OrdRel}\, P$ is strongly reflexive, antisymmetric, and transitive and $\mathrm{OrdRel}\, P$ is respecting addition and respecting multiplication.

Let R be an ordered ring and O be an ordering of R. One can verify that $\mathrm{OrdRel}\, O$ is totally connected.

Let R be a preordered ring. Note that there exists a binary relation on R which is strongly reflexive, antisymmetric, transitive, respecting addition, and respecting multiplication.

Let R be an ordered ring. Note that there exists a binary relation on R which is strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication, and totally connected.

Let R be a preordered ring.

An order relation of R is a strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication binary relation on R. Let R be an ordered ring.

A total order relation of R is a strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication, totally connected binary relation on R. Let R be a ring and Q be a binary relation on R. The functor Positives(Q) yielding a subset of R is defined by the term

(Def. 20) $\{a$, where a is an element of $R : 0_R \leqslant_Q a\}$.

Let R be a preordered ring and Q be a strongly reflexive binary relation on R. One can verify that Positives(Q) is non empty.

Let Q be an order relation of R. Observe that Positives(Q) is closed under addition, closed under multiplication, and negative-disjoint. Let R be an ordered ring and Q be a total order relation of R. One can verify that Positives(Q) is spanning.

Now we state the propositions:

(30) Let us consider a preordered ring R, and a preordering P of R. Then OrdRel P is an order relation of R.

(31) Let us consider an ordered ring R, and an ordering P of R. Then OrdRel P is a total order relation of R.

(32) Let us consider an ordered ring R, and a total order relation Q of R. Then Positives(Q) is an ordering of R.

7. Some Ordered (and Non-ordered) Rings

Let R be a preordered ring. Observe that every subring of R is preordered.

Let R be an ordered ring. One can check that every subring of R is ordered.

Now we state the propositions:

(33) Let us consider a preordered ring R, a preordering P of R, and a subring S of R. Then $P \cap$ (the carrier of S) is a preordering of S.

(34) Let us consider an ordered ring R, an ordering O of R, and a subring S of R. Then $O \cap$ (the carrier of S) is an ordering of S.

Let us observe that $\mathbb{C}_{\mathrm{F}}$ is non preordered. Let n be a non trivial natural number. Let us observe that $\mathbb{Z}/n$ is non preordered.

The functor Positives($\mathbb{R}_{\mathrm{F}}$) yielding a subset of $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 21) $\{r$, where r is an element of $\mathbb{R} : 0 \leqslant r\}$.

One can verify that Positives($\mathbb{R}_{\mathrm{F}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{R}_{\mathrm{F}}$ is ordered.

(35) Positives($\mathbb{R}_{\mathrm{F}}$) is an ordering of $\mathbb{R}_{\mathrm{F}}$.

(36) Let us consider an ordering O of $\mathbb{R}_{\mathrm{F}}$. Then $O =$ Positives($\mathbb{R}_{\mathrm{F}}$). The theorem is a consequence of (24) and (29).

The functor Positives($\mathbb{F}_{\mathbb{Q}}$) yielding a subset of $\mathbb{F}_{\mathbb{Q}}$ is defined by the term

(Def. 22) $\{r$, where r is an element of $\mathbb{Q} : 0 \leqslant r\}$.

Observe that Positives($\mathbb{F}_{\mathbb{Q}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{F}_{\mathbb{Q}}$ is ordered.

(37) Positives($\mathbb{F}_{\mathbb{Q}}$) is an ordering of $\mathbb{F}_{\mathbb{Q}}$.

(38) Let us consider an ordering O of $\mathbb{F}_{\mathbb{Q}}$. Then $O =$ Positives($\mathbb{F}_{\mathbb{Q}}$).

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ \$1 $\in O$. $1_{\mathbb{F}_{\mathbb{Q}}}$, $0_{\mathbb{F}_{\mathbb{Q}}} \in O$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. Positives($\mathbb{F}_{\mathbb{Q}}$) $\subseteq O$ by [6, (1)], (25), [10, (3)], (27). □

The functor Positives($\mathbb{Z}^{\mathrm{R}}$) yielding a subset of $\mathbb{Z}^{\mathrm{R}}$ is defined by the term

(Def. 23) $\{i$, where i is an element of $\mathbb{Z} : 0 \leqslant i\}$.

Note that Positives($\mathbb{Z}^{\mathrm{R}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{Z}^{\mathrm{R}}$ is ordered.

(39) Positives($\mathbb{Z}^{\mathrm{R}}$) is an ordering of $\mathbb{Z}^{\mathrm{R}}$.

(40) Let us consider an ordering O of $\mathbb{Z}^{\mathrm{R}}$. Then $O =$ Positives($\mathbb{Z}^{\mathrm{R}}$).

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ \$1 $\in O$. $1_{\mathbb{Z}^{\mathrm{R}}}$, $0_{\mathbb{Z}^{\mathrm{R}}} \in O$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. □

8. Ordered Polynomial Rings

Let R be a preordered ring and P be a preordering of R. The functor PositPoly(P) yielding a subset of PolyRing(R) is defined by the term

(Def. 24) $\{p$, where p is a polynomial over $R : \mathrm{LC}\, p \in P\}$.

Let R be a preordered, non degenerated ring. Note that PositPoly(P) is closed under addition and negative-disjoint.

Let R be a preordered integral domain. Let us observe that PositPoly(P) is closed under multiplication and has all sums of squares.

Let R be an ordered ring and O be an ordering of R. Let us observe that PositPoly(O) is spanning.

Let R be a preordered integral domain. One can verify that PolyRing(R) is preordered.

Let R be an ordered integral domain. Note that PolyRing(R) is ordered.

Now we state the propositions:

(41) Let us consider a preordered integral domain R, and a preordering P of R. Then PositPoly(P) is a preordering of PolyRing(R).

(42) Let us consider an ordered integral domain R, and an ordering O of R. Then PositPoly(O) is an ordering of PolyRing(R).

Let R be a preordered ring and P be a preordering of R. The functor LowPositPoly(P) yielding a subset of PolyRing(R) is defined by the term

(Def. 25) $\{p$, where p is a polynomial over $R : p(\min^*\{i$, where i is a natural number $: p(i) \neq 0_R\}) \in P\}$.

Let R be a preordered, non degenerated ring. Observe that LowPositPoly(P) is closed under addition and negative-disjoint.

Let R be a preordered integral domain. One can verify that LowPositPoly(P) is closed under multiplication and has all sums of squares.

Let R be an ordered, non degenerated ring and O be an ordering of R. One can check that LowPositPoly(O) is spanning.

Now we state the propositions:

(43) Let us consider a preordered integral domain R, and a preordering P of R. Then LowPositPoly(P) is a preordering of PolyRing(R).

(44) Let us consider an ordered integral domain R, and an ordering O of R. Then LowPositPoly(O) is an ordering of PolyRing(R).

(45) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then PositPoly(P) $\neq$ LowPositPoly(P). The theorem is a consequence of (25) and (26).

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] Nathan Jacobson. *Lecture Notes in Abstract Algebra, III. Theory of Fields and Galois Theory*. Springer-Verlag, 1964.

[5] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*. Vieweg-Verlag, 1989.
[6] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[7] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[8] Alexander Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984.
[9] Knut Radbruch. *Geordnete Körper*. Lecture Notes, University of Kaiserslautern, Germany, 1991.
[10] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

Received March 17, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.