Jan Jakóbowski

SOME EXAMPLES OF DENUMERABLE
PSEUDO-ORDERED FIELDS
AND THEIR APPLICATIONS TO GEOMETRY

Abstract. The paper deals with the following problems concerning pseudo-ordered denumerable fields:

- (i) a connection between Fermat's two squares theorem and the unique pseudo-order in a finite field;
- (ii) properties of a proper pseudo-order determined by any prime number in the field of rational numbers;
- (iii) existence of a proper pseudo-order in every subfield of the sequence used to obtain the field of constructible numbers;
- (iv) some brief of applications of the latter pseudo-orders to construct new algebraic and geometric structures.

In particular, we extend the known construction of finite nearfields or quasifields given by e.g. W. A. Pierce or P. Dembowski – to infinite cases.

1. Preliminary results

DEFINITION 1.1. [4, p. 180, 9, p. 427] A field F is *pseudo-ordered* if a multiplicative subgroup D of index 2 is given in it. An element $q \in F$ is called *positive* if $q \in D$ (then we write $q > 0$) ; *negative* – if $q \notin D$, $q \neq 0$ (then we write $q < 0$).

REMARK 1.2. The notation “ > 0 ” is connected with one multiplicative group of index 2. In the case of more such groups of the same field, we shall use distinct “signs”: > 0 , $>' 0$, etc. Especially, the notation $q \succ 0$ (and consequently $q \prec 0$, $q \succeq 0$, $q \preceq 0$) shall be used for the standard order in the field $\mathcal{R}$ (and its subfields) of real numbers.

2010 *Mathematics Subject Classification*: 11E25; 12F10; 12J15; 51A35; 51B20; 51E15.

Key words and phrases: Fermat's two squares theorem, Minkowski plane, nearfield, quasifield, pseudo-ordered field.

DEFINITION 1.3. [9, p. 428] Let F be a pseudo-ordered field and let $f : F \rightarrow F$. The function f *preserves* (respectively *reverses*) the pseudo-order if

$$(1.1) \quad \frac{f(u) - f(v)}{u - v} > 0 \quad (\text{respectively} \quad \frac{f(u) - f(v)}{u - v} < 0)$$

for every $u, v \in F$, $u \neq v$. Functions preserving or reversing a pseudo-order are called *monotonic*.

COROLLARY 1.4. [6, p. 347]

- a) Every ordered field is pseudo-ordered.
- b) In every pseudo-ordered field
 - all non-zero squares are positive elements;
 - either every element q , $q \neq 0$, satisfies the condition $[q > 0 \Leftrightarrow -q < 0]$ or every element q , $q \neq 0$, satisfies the condition $[q > 0 \Leftrightarrow -q > 0]$.
- c) The field of complex numbers and all finite fields of even order are not pseudo-ordered since every element is a square.

A pseudo-order is *proper* if it is not an order. Let $\mathcal{Q}$, $\mathcal{R}$ and $\mathcal{N}$ denote the field of rational numbers, the field of real numbers, and the set of natural numbers, respectively.

THEOREM 1.5. [7, Theorem 10] For every prime p and for any $n \in \mathcal{N}$ with $n \neq 0$, there exists exactly one (up to isomorphism) field (denoted $GF(p^n)$ and called Galois field) containing exactly p^n elements. Every finite field is isomorphic to some $GF(p^n)$.

THEOREM 1.6. (Fermat's two squares theorem, see [3]) For every prime odd p , the following conditions are equivalent:

- a) There exists $k \in \mathcal{N}$ such that $p = 4k + 1$.
- b) There exist $q, r \in \mathcal{N}$ such that $p = q^2 + r^2$.

Usually the Fermat's two squares theorem is presented as implication $a) \Rightarrow b)$ but very simple calculation gives $b) \Rightarrow a)$ (it suffices to consider all possibilities for $q = 4s + t$, $r = 4u + v$, where $0 \preceq t, v \prec 4$).

Although *nearfields*, *quasifields* [2, p. 129–130] and some other algebraic structures are not so familiar as, e.g. rings or fields, they are widely applied in geometry. Roughly speaking, a *nearfield* is a “field” without left (or right) distributivity; in a *quasifield* the associative law of multiplication does not hold, either (hence the left and the right inverse of an element q do not coincide).

EXAMPLE 1.7. [1], [9, p. 428] In every finite field $GF(p^n)$ with odd p , there exists exactly one pseudo-order and the set of all positive elements coincides

with the set $\mathcal{S}$ of all nonzero squares. The only monotonic mappings are described by

$$(1.2) \quad f(x) = q \cdot \omega(x) + r; \quad q, r \in GF(p^n); \quad \omega \in \text{Aut}(GF(p^n)).$$

The map f preserves (resp. reverses) the pseudo-order if $q > 0$ (resp. $q < 0$). If $GF(p^n)$ admits a nontrivial automorphism φ , then the new multiplication $\bullet$ is defined by

$$(1.3) \quad q \bullet r = \begin{cases} qr & \text{if } r \in \mathcal{S}, \\ \varphi(q)r & \text{if } r \notin \mathcal{S}. \end{cases}$$

Replacing the multiplication from $GF(p^n)$ by $\bullet$, we get a nearfield (quasifield, respectively) if φ is (resp. is not) an involution.

EXAMPLE 1.8. [9, p. 427] In the field $\mathcal{Q}$, every prime number p determines a proper pseudo-order in the following way: every rational number r is uniquely expressible in the form $r = \frac{p^i s}{t}$, where i, s and t are some integers, such that p, s, t are prime to each other. Then for $s \neq 0$, the element r is positive if i is even, and negative if i is odd.

EXAMPLE 1.9. Take $w_1 \in \mathcal{Q}$ such that $\sqrt{w_1} \in \mathcal{R} \setminus \mathcal{Q}$. Then $\mathcal{Q}(\sqrt{w_1}) = \{q + r\sqrt{w_1}; q, r \in \mathcal{Q}\}$ is a subfield in $\mathcal{R}$. Denote $F_0 = \mathcal{Q}$, $F_1 = \mathcal{Q}(\sqrt{w_1})$ and for every $n \in \mathcal{N}$, $n \neq 0$, we take $w_n \in F_{n-1}$ such that $\sqrt{w_n} \in \mathcal{R} \setminus F_{n-1}$ and construct a subfield (of $\mathcal{R}$)

$$(1.4) \quad F_n = F_{n-1}(\sqrt{w_n}) = \{q + r\sqrt{w_n}; q, r \in F_{n-1}\}.$$

Thus we obtain an increasing sequence $F_0 \subset F_1 \subset \dots \subset F_n \subset F_{n+1} \subset \dots$, where F_n is an algebraic extension of F_{n-1} of the 2-nd degree. It is the well known way to get the field $\bigcup_{n=0}^{\infty} F_n$ of real constructible numbers (cf. [10]).

EXAMPLE 1.10. [8, p. 271] For every commutative field F , the *projective line over F* may be treated as the set $\overline{F} = F \cup \{\infty\}$. We extend addition and multiplication from the field F to $\overline{F}$ as follows: $q + \infty = \infty + q = \infty$ for every $q \in \overline{F}$; $q \cdot \infty = \infty \cdot q = \infty$ for every $q \in \overline{F}$, $q \neq 0$. Let $PGL(2, F)$ be the set of all permutations of $\overline{F}$ defined by

$$(1.5) \quad \gamma: x \mapsto \frac{qx + r}{sx + t}, \quad \text{where } q, r, s, t \in F, \quad \det \gamma = qt - rs \neq 0$$

(i.e. the group $PGL(2, F)$ acts on the projective line $\overline{F}$). If we put $\Pi = \overline{F} \times \overline{F}$; $\Sigma_+ = \{(r, y); y \in \overline{F}; r \in \overline{F}\}$; $\Sigma_- = \{(x, r); x \in \overline{F}; r \in \overline{F}\}$; $\Lambda = \{(x, \gamma(x)); x \in \overline{F}; \gamma \in PGL(2, F)\}$, then the structure $(\Pi, \Sigma_+, \Sigma_-, \Lambda)$ is a *Minkowski plane over the field F* . This model is called classical. Elements of Π , Σ_+ , Σ_- and Λ are called *points*, *(+)generators*, *(-)generators* and *circles*, respectively.

2. Properties of chosen pseudo-ordered fields

REMARK 2.1. Every automorphism φ of a pseudo-ordered field maps a subgroup of index 2 onto a subgroup of index 2, but not necessarily the same one. Therefore, in general $q > 0 \not\Rightarrow \varphi(q) > 0$. Moreover, the equivalence $q > 0 \Leftrightarrow \varphi(q) > 0$ does not mean that φ preserves the order (see Remark 1.2 and Proposition 2.10).

The following extends (1.3).

DEFINITION 2.2. For every nontrivial automorphism φ of a pseudo-ordered field F

$$(2.1) \quad q \star r = \begin{cases} qr & \text{for } r > 0, \\ \varphi(q)r & \text{for } r < 0. \end{cases}$$

PROPOSITION 2.3. *If an automorphism φ of a field F satisfies the condition $q > 0 \Leftrightarrow \varphi(q) > 0$, then the set of all elements of F , provided with multiplication $\star$ and initial addition, is a (right-side) quasifield. If additionally φ is an involution then the structure is a nearfield and vice versa.*

Proof. Take $q, r, s \in F$ and denote the inverse of q in the field F by q^{-1} . Since $\varphi(1) = 1 > 0$, we get $q \star 1 = q = 1 \star q$. If $q \star r = 1$ then either $q > 0 \wedge r > 0$ or $q < 0 \wedge r < 0$ (we use the assumption $q > 0 \Leftrightarrow \varphi(q) > 0$). Therefore

$$1 = \begin{cases} qr, & \text{i.e. } q = r^{-1} \text{ and } r = q^{-1} \text{ if } r > 0, \\ \varphi(q)r, & \text{i.e. } q = \varphi^{-1}(r^{-1}) \text{ and } r = (\varphi(q))^{-1} \text{ if } r < 0, \end{cases}$$

and the left inverse of q with respect to $\star$ coincides with the right one iff $\varphi^{-1} = \varphi$.

Consider associativity. We get

$$q \star (r \star s) = \begin{cases} q(rs) & \text{for } r > 0, s > 0, \\ q(\varphi(r)s) & \text{for } r < 0, s < 0, \\ \varphi(q)(\varphi(r)s) & \text{for } r > 0, s < 0, \\ \varphi(q)(rs) & \text{for } r < 0, s > 0, \end{cases}$$

$$(q \star r) \star s = \begin{cases} (qr)s & \text{for } r > 0, s > 0, \\ \varphi(\varphi(q)r)s = (\varphi(\varphi(q))\varphi(r))s & \text{for } r < 0, s < 0, \\ \varphi(qr)s = (\varphi(q)\varphi(r))s & \text{for } r > 0, s < 0, \\ (\varphi(q)r)s & \text{for } r < 0, s > 0. \end{cases}$$

Therefore $q \star (r \star s) = (q \star r) \star s$ if and only if $\varphi(\varphi(q)) = q$. By the way, associativity implies that the left and the right inverse of an element q coincide.

Consider in turn the right and the left distributivity. We get

$$(q + r) \star s = \begin{cases} (q + r)s = qs + rs & \text{for } s > 0, \\ \varphi(q + r)s = \varphi(q)s + \varphi(r)s & \text{for } s < 0, \end{cases}$$

i.e. $(q + r) \star s = q \star s + r \star s$,

$$q \star (r + s) = \begin{cases} q(r + s) & \text{for } r + s > 0, \\ \varphi(q)(r + s) & \text{for } r + s < 0, \end{cases}$$

$$q \star r + q \star s = \begin{cases} qr + qs & \text{for } r > 0, s > 0, \\ \varphi(q)r + \varphi(q)s & \text{for } r < 0, s < 0, \\ qr + \varphi(q)s & \text{for } r > 0, s < 0, \\ \varphi(q)r + qs & \text{for } r < 0, s > 0. \end{cases}$$

Since the “signs” of r , s and $r + s$ are independent, we get $q \star (r + s) \neq q \star r + q \star s$ in every case of distinct “signs”. ■

REMARK 2.4. Definition 2.2 and Proposition 2.3 may be given in dual form

$$(2.2) \quad q * r = \begin{cases} qr & \text{for } q > 0, \\ q\varphi(r) & \text{for } q < 0. \end{cases}$$

Then we get left distributivity, not right.

2.1. Finite pseudo-ordered fields

PROPOSITION 2.5. *In $GF(p^n)$, where p is odd, we have:*

1. $p^n = 4k + 1$ for some $k \in \mathcal{N}$, if and only if for $a \in GF(p^n)$ $a > 0 \Leftrightarrow -a > 0$;
2. $p^n = 4k + 3$ for some $k \in \mathcal{N}$, if and only if for $a \in GF(p^n)$ $a > 0 \Leftrightarrow -a < 0$.

Proof. We have to recall Corollary 1.4b) and Example 1.7. Of course, the items 1. and 2. are equivalent since either $p^n = 4k + 1$ or $p^n = 4k + 3$. The condition $a > 0 \Leftrightarrow -a > 0$ yields to partition of all elements except 0 onto four subsets of the same cardinality. Thus we have proved “only if” in 1. Consider the case $p^n = 4k + 1$. Then either n is arbitrary and $p = 4s + 1$ for some $s \in \mathcal{N}$, or n is even and $p = 4s + 3$. Let $n = 1$. By the Fermat’s two squares theorem, $p = 4k + 1$ means $p = q^2 + r^2$ for some $q, r \in \mathcal{N}$. Hence $q^2 = -r^2$ in $GF(p)$, where $q^2, r^2 > 0$. Consider arbitrary n and assume $p = 4s + 1$. Since $GF(p)$ is a subfield of $GF(p^n)$ and $u > 0 \Leftrightarrow -u > 0$ in $GF(p)$, this property holds in all $GF(p^n)$. If $p = 4s + 3$ and $n = 2$, then by Theorem 1.5, $GF(p^2)$ is isomorphic with the extension $GF(p)(j)$, where $j^2 = v$ for some $v \in GF(p)$, such that v is not a square in $GF(p)$. We

already know that in $GF(p)$ $v < 0$ and $-v > 0$. Certainly, $-v$ is a square in $GF(p^2)$ but so is v . Therefore in $GF(p^2)$ $v > 0$ and $-v > 0$. If $p = 4s + 3$ and $n = 2m$ for some $m \in \mathcal{N}$, then $GF(p^n)$ is an extension of $GF(p^2)$, where $u > 0 \Leftrightarrow -u > 0$. ■

COROLLARY 2.6. *In any Galois field $GF(p^n)$, with odd p , the element -1 is a square iff $p^n = 4k + 1$ for some $k \in \mathcal{N}$.*

REMARK 2.7. An equality $q^2 + r^2 = 0$ in $GF(p^n)$ does not mean that the number p^n is a sum of two nonzero squares, e.g. $49 \neq q^2 + r^2$ for every $q, r \in \mathcal{N} \setminus \{0\}$.

2.2. Proper pseudo-order in the field of rational numbers

PROPOSITION 2.8. *The pseudo-order, determined in $\mathcal{Q}$ by any prime p , has the following properties:*

1. For every $v \in \mathcal{Q}$, $v > 0 \Leftrightarrow -v > 0$.
2. There exist positive elements which are not squares.
3. Every prime number q is positive if and only if $q \neq p$.
4. Bijections $f(\frac{p^i u}{v}) = \frac{p^{-i} u}{v}$ and $g(\frac{p^i u}{v}) = \frac{p^{-i} v}{u}$ preserve the sets of positive and of negative elements but they are not monotonic.

Proof. The items 1. and 2. are obvious.

Ad 3. Note that $p = \frac{p^1 \cdot 1}{1}$ and $q = \frac{p^0 \cdot q}{1}$.

Ad 4. Certainly, f is a bijection preserving the sets of positive and of negative elements. Take elements $r = \frac{p^i u}{v}$, $s = \frac{p^i w}{z}$, where i is odd, u, v, w, z are prime to each other, and we get

$$(2.3) \quad \frac{f(r) - f(s)}{r - s} = \frac{p^{-i}(\frac{u}{v} - \frac{w}{z})}{p^i(\frac{u}{v} - \frac{w}{z})} = p^{-2i} > 0,$$

$$(2.4) \quad \frac{f(r) - f(p^i r)}{r - p^i r} = \frac{\frac{p^{-i} u}{v} - \frac{p^{-2i} u}{v}}{\frac{p^i u}{v} - \frac{p^{2i} u}{v}} = p^{-3i} \cdot (-1) < 0.$$

In the same way we consider g . ■

EXAMPLE 2.9. The involutorial bijections f and g , considered above, are not automorphisms of the field of rational numbers but they are automorphisms of the multiplicative subgroup $(\mathcal{Q} \setminus \{0\}, \cdot)$. Hence, the structure $(\mathcal{Q}, +, \star)$, where $\star$ is the same as in (2.1) with $\varphi := f$, satisfies all conditions to be a field, except neither left nor right distributivity. Here work the same arguments as in Proposition 2.3.

2.3. Pseudo-order in subfields of the field of real constructible numbers

PROPOSITION 2.10. *For every $n \in \mathcal{N} \setminus \{0\}$, the field F_n defined by (1.4) has two orders and at least one proper pseudo-order. The involutorial automorphism $\varphi_n(q + r\sqrt{w_n}) = q - r\sqrt{w_n}$ changes the orders and preserves the proper pseudo-order.*

Proof. The first order is standard, i.e. $q + r\sqrt{w_n} \succ 0$ iff $q \succ -r\sqrt{w_n}$ (see Remark 1.2 for notations), in the second one we put $q + r\sqrt{w_n} \succ' 0$ iff $q \succ r\sqrt{w_n}$ and certainly it is an order. For the proper pseudo-order we put $q + r\sqrt{w_n} > 0$ iff $q^2 \succ r^2 w_n$. Let us consider the latter case. We get

$$(q + r\sqrt{w_n})(s + t\sqrt{w_n}) = qs + rtw_n + (qt + rs)\sqrt{w_n},$$

and

$$(qs + rtw_n)^2 - (qt + rs)^2 w_n = (q^2 - r^2 w_n)(s^2 - t^2 w_n).$$

Therefore $\{q + r\sqrt{w_n}; q^2 \succ r^2 w_n\}$ is a multiplicative subgroup of index 2. This pseudo-order is proper since, for every $q, r \in F_{n-1}$ such that $q^2 \succ r^2 w_n$, we have $(q + r\sqrt{w_n}) + (-q + r\sqrt{w_n}) = 0 + 2r\sqrt{w_n}$ and $0^2 \prec 4r^2 w_n$. Thus, the sum of two positive elements may be negative.

Now the part concerning φ_n is clear. ■

From Propositions 2.3 and 2.10 the following is immediate

COROLLARY 2.11. *For every $n \in \mathcal{N}$, there exists a nearfield $\mathcal{N}_n$ with the set of elements and addition defined as in the field F_n and multiplication $\star$ defined by*

$$(q + r\sqrt{w_n}) \star (s + t\sqrt{w_n}) = \begin{cases} (q + r\sqrt{w_n})(s + t\sqrt{w_n}) & \text{for } s^2 \succ t^2 w_n, \\ (q - r\sqrt{w_n})(s + t\sqrt{w_n}) & \text{for } s^2 \prec t^2 w_n. \end{cases}$$

In accordance with Remark 2.4, dual definition is also possible

$$(q + r\sqrt{w_n}) * (s + t\sqrt{w_n}) = \begin{cases} (q + r\sqrt{w_n})(s + t\sqrt{w_n}) & \text{for } q^2 \succ r^2 w_n, \\ (q + r\sqrt{w_n})(s - t\sqrt{w_n}) & \text{for } q^2 \prec r^2 w_n. \end{cases}$$

3. Some geometric structures related to pseudo-ordered fields F_n

It is not the aim of this paper to give an exhausting description of geometric structures and their specific properties. We shall only mention that existence of pseudo-ordered denumerable fields with monotonic functions yields construction of some geometric structures, i.e. Minkowski planes, projective planes, nearaffine planes, which are not classical. Each of such a structure consists of a denumerable point set provided with some families of subsets satisfying a number of conditions (for precise definitions see, e.g. [2, 8, 11]). One of the constructions, giving a wide family of

nonclassical Minkowski planes, is the following. If a field F is pseudo-ordered then we obtain $\text{PGL}(2, F) = \text{PGL}^+(2, F) \cup \text{PGL}^-(2, F)$, where $\gamma \in \text{PGL}^+(2, F) \Leftrightarrow \det(\gamma) > 0$ (cf. Example 1.10). For pairwise distinct $x_1, x_2, x_3 \in \bar{F}$ let us denote [4, p. 181]:

$$(3.1) \quad \delta(x_1, x_2, x_3) = \begin{cases} (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) & \text{for } x_1, x_2, x_3 \in F, \\ x_3 - x_2 & \text{for } x_1 = \infty, \\ x_1 - x_3 & \text{for } x_2 = \infty, \\ x_2 - x_1 & \text{for } x_3 = \infty. \end{cases}$$

Then, having non-constant mappings $f, g : \bar{F} \rightarrow \bar{F}$, such that $f(\infty) = g(\infty) = \infty$, we simply replace the family Λ of circles of the classical Minkowski plane over F (see Example 1.10), by $\Lambda(f, g) = \Lambda_1 \cup \Lambda_2(f, g)$, where

$$\Lambda_1 = \{(x, \gamma(x)); x \in \bar{F}; \gamma \in \text{PGL}^+(2, F)\},$$

$$\Lambda_2(f, g) = \{(x, y); g(y) = \gamma(f(x)), x \in \bar{F}; \gamma \in \text{PGL}^-(2, F)\},$$

subject to the condition that f and g be chosen so as to make $\Lambda_1 \cap \Lambda_2(f, g) = \emptyset$. We preserve unchanged sets Π, Σ_+, Σ_- of the classical Minkowski plane over F and obtain the following theorem.

THEOREM 3.1. [4, p. 181] $\Lambda_1 \cap \Lambda_2(f, g) = \emptyset$ and $\mathbf{M}_{f,g}(F) = (\Pi, \Sigma_+, \Sigma_-, \Lambda(f, g))$ is a Minkowski plane if and only if the following conditions hold:

- (I) $\delta(f(x_1), f(x_2), f(x_3)) \cdot \delta(g(y_1), g(y_2), g(y_3)) \delta(x_1, x_2, x_3) \cdot \delta(y_1, y_2, y_3) > 0$ for every two pairwise distinct triples $x_1, x_2, x_3 \in \bar{F}$ and $y_1, y_2, y_3 \in \bar{F}$;
- (II) f and g are bijections;
- (III) $|Fix(\gamma_1 \circ g^{-1} \circ \gamma_2 \circ f)| \neq 1$ for every $\gamma_1 \in \text{PGL}^+(2, F)$ and every $\gamma_2 \in \text{PGL}^-(2, F)$ ($|Fix(\gamma)|$ denotes a number of points fixed by γ).

PROPOSITION 3.2. For every field F_n with proper pseudo-order described in Proposition 2.10, the pairs of functions $\varphi_n(q+r\sqrt{w_n}) = q-r\sqrt{w_n}$, $g_n = id_{F_n}$ and $f_n(q+r\sqrt{w_n}) = -q+r\sqrt{w_n}$, $g_n = id_{F_n}$, satisfy the conditions (I)–(III) of Theorem 3.1.

Proof. The conditions (II) and (III) are obvious since φ_n is an (involutorial) automorphism of F_n , $f_n = -1 \cdot \varphi_n$ and $-1 > 0$, and $|Fix(\gamma_1 \circ \gamma_2)| \neq 1$. To prove (I), note that, e.g. $\delta(f_n(q_1+r_1\sqrt{w_n}), f_n(q_2+r_2\sqrt{w_n}), f_n(q_3+r_3\sqrt{w_n})) \cdot \delta(q_1+r_1\sqrt{w_n}, q_2+r_2\sqrt{w_n}, q_3+r_3\sqrt{w_n}) = (-q_1+r_1\sqrt{w_n})(q_1+r_1\sqrt{w_n})(-q_2+r_2)(q_2+r_2)(-q_3+r_3\sqrt{w_n})(q_3+r_3\sqrt{w_n}) = (-q_1^2+r_1^2w_n)(-q_2^2+r_2^2w_n)(-q_3^2+r_3^2w_n) > 0$. ■

For any geometrical structure one may consider so-called internal or external structures with respect to some point P [2, p. 3]. Roughly speaking, we reject P and all blocks through P to obtain the external structure. Similarly, we get the internal structure with respect to P if we reject P and all blocks not passing through P . In the case of Minkowski planes, there are two kinds of blocks (circles and generators). The modified external structure with respect to the point P is called the residual plane [12, p. 120–123] and it satisfies all axioms of a nearaffine plane [11, p. 53–54]. Then traces of circles not through P become *proper lines* and traces of generators not through P are *straight lines*. Modification is that we reject not only one point P but all points lying on generators through P . If we take a mixed structure with the same point set as before, traces of all circles through P and traces of all generators not through P , then we get so-called derived plane which satisfies all axioms of an affine plane [8, p. 273]. In particular, taking $P = (\infty, \infty)$, we get

PROPOSITION 3.3. [5, p. 244], [4, p. 187] *If for some functions f, g acting on a pseudo-ordered field F , there exists the Minkowski plane $\mathbf{M}_{f,g}(F)$, then there also exist the nearaffine plane $\Theta_{f,g}(F)$ and the affine plane $\mathbf{C}_{f,g}(F)$.*

COROLLARY 3.4. *For every $n \in \mathcal{N}$, there exist the affine plane $\mathbf{C}_{\varphi_n, id_{F_n}}(F_n)$ and the nearaffine plane $\Theta_{\varphi_n, id_{F_n}}(F_n)$ constructed over a nearfield.*

We can obtain affine planes $\mathbf{C}_{f,g}(F)$ [5, p. 244] and nearaffine planes $\Theta_{f,g}(F)$ [6, pp. 348–349] related to pseudo-ordered fields, independently of Minkowski planes. In the case of affine planes, we replace the classic lines $y = mx + n$ with negative slope m by the sets of points (x, y) satisfying $g(y) = mf(x) + n$. In the case of nearaffine planes, classic proper lines $(x-p)(y-q) = r$ with $-r > 0$ are replaced by the sets $(f(x)-p)(g(y)-q) = r$. Of course, the conditions (I)–(III) of Theorem 3.1 are replaced by some other version. Certainly, all lines of $\mathbf{C}_{\varphi_n, id_{F_n}}(F_n)$ may be presented as $y = m * x + n$. If one considers $\mathbf{D}_{\varphi_n, id_{F_n}}(F_n)$ with the same point set and lines given by $y = m \star x + n$, then the projective extensions of $\mathbf{C}_{\varphi_n, id_{F_n}}(F_n)$ and $\mathbf{D}_{\varphi_n, id_{F_n}}(F_n)$ are dual to each other [2, p. 116]. Proper lines of the nearaffine plane $\Theta_{\varphi_n, id_{F_n}}(F_n)$ are given by $y = s * (x - q)^{-1} + r$, where t^{-1} means the inverse of t in the field F_n .

For all mappings f and g acting on $\overline{F}$, such that f, g satisfy the conditions (I) – (III) of Theorem 3.1, one can define multiplicative operations in the same way as $*$ and $\star$, preserve addition from F and get some algebraic structure. Such structures are described in e.g. [2, pp. 124–126].

References

- [1] L. Carlitz, *A theorem on permutations in a finite fields*, Proc. Amer. Math. Soc. 11 (1966), 456–459.
- [2] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin-Heidelberg-New York, 1968.
- [3] J. A. Ewell, *A simple proof of Fermat's two squares theorem*, Amer. Math. Monthly 90 (1983), 635–637.
- [4] J. Jakóbowski, *A new construction for Minkowski planes*, Geom. Dedicata 69 (1998), 179–188.
- [5] J. Jakóbowski, *A new generalization of Moulton affine planes*, Geom. Dedicata 42 (1992), 243–253.
- [6] J. Jakóbowski, *Nearaffine planes related to pseudo-ordered fields*, Bull. Polish Acad. Sci. Math. 50 (2002), 345–360.
- [7] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 1970.
- [8] N. Percsy, *Finite Minkowski planes in which every circle-symmetry is an automorphism*, Geom. Dedicata 10 (1981), 269–282.
- [9] W. A. Pierce, *Moulton planes*, Canad. J. Math. 13 (1961), 427–436.
- [10] C. R. Videla, *On the constructible numbers*, Proc. Amer. Math. Soc. 127 (1999), 851–860.
- [11] H. A. Wilbrink, *Nearaffine planes*, Geom. Dedicata 12 (1982), 53–62.
- [12] H. A. Wilbrink, *Finite Minkowski planes*, Geom. Dedicata 12 (1982), 119–129.

UNIVERSITY OF WARMIA AND MAZURY IN OLSZTYN
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
10-710 OLSZTYN, POLAND
E-mail: jjakob@matman.uwm.edu.pl

Received January 21, 2011; revised version October 18, 2011.