On Recent Developments of Planar Nearrings

Wen-Fong Ke

September 12, 2003

– Typeset by FoilTEX –

Definition and examples

Let $(N, +, \cdot)$ be a (left) nearring. Define an equivalence relation $\equiv_m$ on N by

$$a \equiv_m b \Leftrightarrow ax = bx \text{ for all } x \in N.$$

We say that $(N, +, \cdot)$ is *planar* if $|N/\equiv_m| \geq 3$, and for each triple $a, b, c \in N$ with $a \not\equiv_m b$, the equation $ax = bx + c$ has a unique solution for x in N.

- All fields and finite nearfields are planar.

- The three examples [1].

  For $a, b \in \mathbb{C}$, define

$$a *_1 b = \begin{cases} a_1 \cdot b & \text{if } a_1 \neq 0, \\ a_2 \cdot b & \text{if } a_1 = 0; \end{cases}$$

$$a *_2 b = |a| \cdot b;$$

$$a *_3 b = \begin{cases} \dfrac{a}{|a|} \cdot b & \text{if } a \neq 0, \\ 0 & \text{if } a = 0. \end{cases}$$

Then $(\mathbb{C}, +, *_1)$, $(\mathbb{C}, +, *_2)$, and $(\mathbb{C}, +, *_3)$ are planar nearrings which are not rings.

Constructions

A. Planar nearrings ⇝ Ferrero pairs [9]:

Let N be a planar nearring. For $a \in N$ with $a \not\equiv_m 0$, define

$$\varphi_a : N \to N ; x \mapsto ax \quad \text{for all } x \in N.$$

Then

- $\varphi_a \in \mathrm{Aut}(N, +)$, and $\varphi_a \neq 1 \iff a \not\equiv_m 1$
- $\varphi_a(x) = x$ if and only if $\varphi_a = 1$ or $x = 0$.
- $-1 + \varphi_a$ is surjective if $\varphi_a \neq 1$

Thus, $\Phi = \{\varphi_a \mid a \in N, a \not\equiv_m 0\}$ is a regular group of automorphisms of $(N, +)$ with the property that $-1 + \varphi_a$ is surjective if $\varphi_a \neq 1$. We call (N, Φ) a *Ferrero pair*.

In general, if Φ is a group acting on N as an automorphism group, and for $\varphi \in \Phi \setminus \{1\}$, $-1 + \varphi$ is bijective, then (N, Φ) is called a *Ferrero pair*.

B. Ferrero Pair ⇝ Planar nearring:

Let (N, Φ) be a Ferrero pair. Let C be a complete set of orbit representatives of Φ in N. Let $E \subseteq C\setminus\{0\}$ with $|E| \geq 2$. Then

$$N = \cup_{e\in E}\Phi(e) \bigcup \cup_{f\in C\setminus E} \Phi(f).$$

Define $*$ on N by

$$\varphi(e) * y = \begin{cases} \varphi(y) & e \in E, \varphi \in \Phi, y \in N, \\ 0 & \text{otherwise.} \end{cases}$$

Then $(N, +, *)$ is a planar nearring.

- ◇ The elements in E are exactly the left identities of N.
- ◇ N is an integral planar nearring if and only if $E = C \setminus \{0\}$, .

Examples.

(a) $(\mathbb{C}, +, *_1)$; the corresponding Ferrero pair is $(\mathbb{C}, \widehat{\mathbb{R}}^*)$, where $\widehat{\mathbb{R}}^* = \{\varphi_r \mid r \in \mathbb{R} \setminus \{0\}\}$.

(b) $(\mathbb{C}, +, *_2)$; the corresponding Ferrero pair is $(\mathbb{C}, \widehat{\mathbb{R}}^+)$, where $\widehat{\mathbb{R}}^+ = \{\varphi_r \mid r > 0\}$.

(c) $(\mathbb{C}, +, *_3)$; the corresponding Ferrero pair is $(\mathbb{C}, \widehat{C})$, where $\widehat{C} = \{\varphi_c \mid |c| = 1\}$.

(d) Let F be a field. Then F is a planar nearring. Take $\tilde{\Phi} \leq F^* = F \setminus \{0\}$ and put $\Phi = \{\varphi_a \mid a \in \tilde{\Phi}\} \leq \mathrm{Aut}(F, +)$ where each $\varphi_a : F \to F$ is the left multiplication by a. Then (F, Φ) is a Ferrero pair. Any nearring constructed from (F, Φ) is said to be *field generated*.

Isomorphism problem. Given a Ferrero pair (N, Φ), is there a way to distinguish the planar nearrings constructed from it?

Example. Consider the Ferrero pair $(\mathbb{C}, \widehat{C})$. Take as orbit representatives the sets

$$E_1 = \{x + x^2 i \mid x > 0\} \text{ and } E_2 = \{x \mid x > 0\}.$$

Then the planar nearrings $(\mathbb{C}, +, *_{E_1})$ and $(\mathbb{C}, +, *_{E_2})$ constructed using E_1 and E_2, respectively, are not isomorphic:

Assume that σ is an isomorphism between $N_1 = (\mathbb{C}, +, *_{E_1})$ and $N_2 = (\mathbb{C}, +, *_{E_2})$. Then $\sigma(E_1) = \sigma(E_2)$ as they are the sets of left identities of N_1 and N_2, respectively. Take $3 + 5i \in N_1$. Then

$$\begin{aligned}\sigma(3+5i) &= \sigma((1+i)+(2+4i)) \\ &= \sigma(1+i)+\sigma(2+4i).\end{aligned}$$

- $3 + 5i \notin E_1 \Rightarrow \sigma(3+5i) \notin E_2$.
- $1 + i$ and $2 + 4i \in E_1 \Rightarrow \sigma(1+i), \sigma(2+4i) \in E_2$.
- Since E_2 is closed under $+$, $\sigma(1+i) + \sigma(2+4i) \in E_2$, a contradiction.

Theorem 1. *Let (M, Ψ) and (N, Φ) be Ferrero pairs and let E_1 and E_2 be sets of orbit representatives of Ψ and Φ in M and N, respectively, with $|E_1| \geq 2$. Let $(M, +, \cdot)$ and $(N, +, \star)$ be the planar nearrings defined on M and N using E_1 and E_2, respectively. Then an additive isomorphism σ from $(M, +)$ to $(N, +)$ is an isomorphism of the planar nearrings $(M, +, \cdot)$ and $(N, +, \star)$ if and only if $\sigma(E_1) = E_2$ and $\sigma\Psi\sigma^{-1} = \Phi$.*

In particular, if $(M, \Psi) = (N, \Phi)$, then an automorphism $\sigma \in \mathrm{Aut}(N, +)$ is an isomorphism of N_1 and N_2 if and only if $\sigma(E_1) = E_2$ and σ normalizes Φ.

Remark. This theorem is valid for Ferrero nearring constructions.

Let G be a group and $\Phi \leq \mathrm{Aut}G$. Let A be a complete set of orbit representatives of Φ in G. Suppose that $E \subseteq A$. If $E = \varnothing$, then we have trivial multiplication on G. If $E \neq \varnothing$, we want E to satisfy

$$\varphi(e) \neq e \quad \text{for all } \varphi \in \Phi \setminus \{1\} \text{ and } e \in E.$$

Put $A^\circ = A \setminus E$ and $G^\circ = \Phi A^\circ$. For $x, y \in G$, define

$$x * y = \begin{cases} 0 & \text{if } x \in G^\circ; \\ \varphi(y) & \text{if } x = \varphi(e) \in \Phi E. \end{cases}$$

Then $(G, +, *)$ is a *Ferrero nearring* which is planar if and only if (G, Φ) is a Ferrero pair.

Lemma 2. *Let $\sigma : \mathbb{C} \to \mathbb{C}$ be an automorphism of the additive group $(\mathbb{C}, +)$. If $\sigma^{-1}\widehat{C}\sigma = \widehat{C}$, then σ is either a rotation or a reflection about a line through the origin. Consequently, $\sigma(C) = C$.*

Example. Let E_1 and E_2 be two complete sets of orbit representatives of $\widehat{C}$ in $\mathbb{C} \setminus \{0\}$. Let $\sigma \in \mathrm{Aut}(\mathbb{C}, +)$. If σ is an isomorphism of the planar nearrings, then σ takes C to C. Thus, according to the above lemma, we have that $(\mathbb{C}, +, *_{E_1})$ and $(\mathbb{C}, +, *_{E_2})$ are isomorphic if and only if $E_2 = e^{i\theta}E_1$ or $E_2 = e^{i\theta}\overline{E_1}$ for some $\theta \in \mathbb{R}$.

Questions. (1) Now that we are able to distinguish the planar nearrings defined on $(\mathbb{C}, +)$ using $\widehat{C}$, what's next?

(2) Note that if E is a complete set of orbit representatives of $\widehat{C}$ in $\mathbb{C} \setminus \{0\}$. Then the planar nearring $(\mathbb{C}, +, *_E)$ is a topological nearring if and only if E is a continuous curve in $\mathbb{C}$. Is there a way to characterize them?

Characterizations of Planar Nearrings

Theorem 3 ([3]). *Let N be a zero-symmetric 3-prime nearring. Let L be an N-subgroup of N. Then there is an $e = e^2 \in N$ such that $L = eN$. Let $\Phi = eNe \setminus \{0\}$, then (L, Φ) is a Ferrero pair, and L is a planar nearring.*

Theorem 4 ([17]). *Let P be a (right) planar nearring with corresponding Ferrero pair (P, Φ). Let $N = M_{\Phi}(P)$. Then P is isomorphic to a subnearring $\overline{P}$ with right identity of N such that N is 2-primitive on $\overline{P}$ via the nearring multiplication, and $P \cong \overline{P}$.*

Theorem 5 ([18]). *Let P be a (right) nearring. The P is planar if and only if P is isomorphic to a centralizer sandwich nearring $M(\phi, id, X, N) = \{f : X \to N \mid f(\alpha(x)) = \alpha(f(x))$ for all $\alpha \in C$ and $x \in X\}$. Here C is a fixed point free automorphism group of automorphisms of $(N, +)$ with the following properties:*

(1) *(N, C) is a Ferrero pair;*

(2) *$|X| \geq 2$ and $X = C(a) \cup \{0\}$ for some $a \in N$;*

(3) *the function ϕ acts as the identity map on $C(a)$ and commutes with elements of C.*

Designs from Planar Nearrings

Definition. A set $\boldsymbol{X}$ with $\boldsymbol{v}$ elements together with a family **S** of $\boldsymbol{k}$-subsets of $\boldsymbol{X}$ is called a *balanced incomplete block design* (*BIBD*) if

(i) each element belongs to exactly $\boldsymbol{r}$ subsets, and

(ii) each pair of distinct elements belongs to exactly λ subsets.

The $\boldsymbol{k}$-subsets in **S** are called *blocks*, and the integers $\boldsymbol{v}, \boldsymbol{b} = |\mathbf{S}|, \boldsymbol{r}, \boldsymbol{k}, \lambda$ are referred to as the *parameters* of the BIBD.

(A) **B**, **B**$^-$, **B***

Let (N, Φ) be a finite Ferrero pair (i.e. N is finite). Denote $\Phi^0 = \Phi \cup \{0\}$ and $\Phi^- = \Phi \cup (-\Phi) \cup \{0\}$. Let

$\mathbf{B} = \{\Phi^0 a + b \mid a, b \in N, a \neq 0\}$ where

$$\Phi^0 a + b = \{\Phi(a) + b \mid \Phi \in \Phi^0\};$$

$\mathbf{B}^- = \{\Phi^- a + b \mid a, b \in N, a \neq 0\}$;

$\mathbf{B}^* = \mathbf{B}_\Phi = \{\Phi a + b \mid a, b \in N, a \neq 0\}$;

Theorem 6 ([7]). *Let* (N, Φ) *be a finite Ferrero pair. Then* $(N, \mathbf{B}^*)$ *a BIBD.*

(B) **Conjecture (Modisett).** The automorphism group of (N, B_{Φ}) is the normalizer of Φ in Aut$(N, +)$.

(C) Actually, $(N, +, B_{\Phi})$ is a *design group*, i.e. N has a group structure, and each of the mappings $\rho_a : N \to N ; x \to x + a$, $a \in N$, is an automorphisms of the design. In this case, a mapping $N \to N$ is called an *automorphism* of the design group if it is at the same time an automorphism of the groups as well as of the design.

Theorem 7 ([10]). *Let (N, Φ) be a finite Ferrero pair such that N and Φ are abelian with $|\Phi| < |N| - 1$. Then* Aut$(N, +, B_{\Phi})$ *is the normalizer of Φ in* Aut$(N, +)$.

Theorem 8 ([5]). *Let (M, Ψ) and (N, Φ) be finite Ferrero pair and let σ be an isomorphism from $(M, \mathrm{B}_\Psi, +)$ to $(N, \mathrm{B}_\Phi, +)$. Let $|\Phi| = k$ and set $s = 2k^2 - 6k + 7$. If $|N/[N, N]| > s$, then $\sigma\Psi\sigma^{-1} = \Phi$. In particular, if $(M, \Psi) = (N, \Phi)$, then σ is a normalizer of Φ.*

Example. Let $F = \mathrm{GF}(7^3)$ and $\kappa : F \to \mathrm{Aut}(F)$ a coupling on F such that $F^\kappa := (F, +, \circ)$ is a proper nearfield with $a \circ b := a \cdot \kappa_a(b)$. Let $\Phi \leq F^*$ of index 2. Since Φ is characteristic, $\Phi^\kappa := (\Phi, \circ)$ is a subgroup of $(F^\kappa)^*$. Then Φ^κ is nonabelian, and so Φ and Φ^κ are not isomorphic; therefore Φ and Φ^κ cannot be conjugate to each other. But $(F, \mathrm{B}_\Phi) = (F, \mathrm{B}_{\Phi^\kappa})$.

(D) ([8], [16]) Segments Let (N, Φ) be a Ferrero pair. For distinct $a, b \in N$, define

$$\overline{a, b} = \Phi^0(b - a) + a \cap \Phi^0(a - b) + b,$$

and call it a *segment* with endpoints a and b. Let

$$\mathrm{S} = \{\overline{a, b} \mid a, b \in N, a \neq b\}.$$

Note that if one put $S = \Phi^0 \cap (1 - \Phi^0)$, then $1 - S = S$ and $\overline{a, b} = (b - a)S + a$.

Theorem 9 (H.-M. Sun 2002). *If N is a nearfield or a ring, then $\overline{a, b} = \overline{c, d}$ if and only if $(a, b) = (c, d)$.*

- Field generated cases

Let $F = \mathrm{GF}(q)$ be a Galois field and S a subset of F with $|S| \geq 2$. Consider

$$\mathbf{S} = \{Sa + b \mid a, b \in F, a \neq 0\}.$$

Then $(F, \mathbf{S})$ is always a BIBD.

Theorem 10 ([6]). *If $|S| = 3$, then the $(F, \mathbf{S})$ is a 2-$(q, 3, \lambda)$ design with $\lambda \in \{1, 2, 3, 6\}$. Let $U = \{r \mid \{0, 1, r\} \in \mathbf{S}\}$ and $K = \langle U, +, \cdot\rangle$ be the subfield of F generated by U. Then under some mild condition, we have that $f \in \mathrm{Aut}(F, \mathbf{S})$ if and only if $f(x) = A(\alpha(x)) + b$ $(x \in F)$ for some $b \in F$, $\alpha \in \mathrm{Aut}_K(F)$, and $A \in \mathscr{L}(F, K)$ (= linear transformations of the vector space F over K).*

- Ring generated cases

Let $(R, +, \cdot)$ be a finite ring with unity and denote by $\mathscr{U}(R)$ the group of units of R. Suppose that Φ is a subgroup of $\mathscr{U}(R)$ with $-1 \in \Phi$. Let $\{s_1, \ldots, s_m\}$ be a complete set of orbit representatives of Φ in $R \setminus \{0\}$. For each i, let $A_i = \{\{x, y\} \mid x - y \in \Phi s_i\}$, and set $\mathscr{A} = \{A_i \mid 1 \le i \le m\}$.

Theorem 11 ([16]). (1) $(R, \mathscr{A})$ *is an associative scheme.*

(2) *For any proper subset* S *of* R *with* $|S| \ge 2$, *denote* $\mathsf{S} = \{aS + b \mid a \in \Phi, b \in R\}$. *Then* $(R, \mathsf{S}, \mathscr{A})$ *is a PBIBD.*

Circularity and Graphs

- Definition

$(N, +, \cdot)$: planar nearring, $N^* = \{n \in N \mid n \not\equiv_m 0\}$.

$a, c, b, d \in N$, $a \not\equiv_m 0$, $c \not\equiv_m 0$:

$$N^*a + b \neq N^*c + d \Rightarrow |N^*a + b \cap N^*c + d| \leq 2,$$

then we said that N is *circular*. If (N, Φ) is the corresponding Ferrero pair, then $N^*a = \Phi a = \{\varphi(a) \mid \varphi \in \Phi\}$. So N is circular if $|\Phi a + b \cap \Phi c + d| \leq 2$ for all $a, b, c, d \in N$ with $a \neq 0$, $c \neq 0$ and $\Phi a + b \neq \Phi c + d$. We say that the Ferrero pair (N, Φ) is *circular* in this manner.

Example. $(\mathbb{C}, +, *_3)$ is a circular planar nearring.

- Characterization of circular Ferrero pairs

1. Abelian Φ

   Example. Let $F = \mathrm{GF}(p^2)$, p a prime, and let Φ_{p+1} be the subgroup of F^*. Then the Ferrero pair (F, Φ_{p+1}) is circular. Consequently, if $k \geq 3$ and p is a prime with $k \mid (p+1)$, then the Ferrero (F, Φ_k) is circular.

   Theorem 12 ([13]). *For each $k \geq 3$, there is a nonempty finite subset $\mathscr{P}_k$ of prime numbers with the following property: Let $q = p^s$, a power of some prime p, be such that $k \mid (q-1)$. Then there is a subgroup Φ_k of the multiplicative group $\mathrm{GF}(q)^*$, and the Ferrero pair $(\mathrm{GF}(q), \Phi_k)$ is circular if and only if $p \in \mathscr{P}_k$.*

Question. For practical applications, an upper bound of $\mathscr{P}_k$ in terms of k will be useful. Can we do so?

Let $\zeta = e^{2\pi i/k} \in \mathbb{C}$. For u, v, s, t with $1 \leq u < v \leq s \leq k-1$, $1 \leq t \leq k-1$, and $v \neq t$ and $s \neq t$, define $\varphi_{u,v,s,t} = (\zeta^u - 1)(\zeta^t - 1) - (\zeta^v - 1)(\zeta^s - 1) \in \mathbb{Z}[\zeta]$. Then $\varphi_{u,v,s,t}$ is nonzero and has integer norm. The set $\mathscr{P}_k$ consists of the prime factors of the norms $N_{\mathbb{Q}(\zeta):\mathbb{Q}}(\varphi_{u,v,s,t})$ of all such $\varphi_{u,v,s,t}$. Since $\varphi_{u,v,s,t}$ expands to 6 summands of powers of ζ, we see that the norm is less than or equal $6^{\varphi(k)}$, where $\varphi(k)$ is the Euler totient function giving the number of automorphisms of the k-th cyclotomic field.

Conjecture: $N_{\mathbb{Q}(\xi):\mathbb{Q}}(\varphi_{u,v,s,t}) \leq (8\sqrt{3}/3)^{\varphi(k)}$.

$\mathscr{P}_4 = \{2, 5\}$,

$\mathscr{P}_5 = \{5, 11\}$,

$\mathscr{P}_6 = \{2, 3, 7, 13, 19\}$,

$\mathscr{P}_7 = \{2, 7, 29, 43\}$,

$\mathscr{P}_8 = \{2, 3, 5, 17, 41\}$,

$\mathscr{P}_9 = \{3, 19, 37, 73, 109, 127, 271\}$,

$\mathscr{P}_{10} = \{2, 5, 11, 31, 41, 61, 71, 101\}$,

$\mathscr{P}_{11} = \{11, 23, 67, 89, 199, 353, 397, 683\}$,

$\mathscr{P}_{12} = \{2, 3, 5, 7, 13, 17, 19, 37, 61, 73, 97, 109, 157, 181, 193\}$.

Question. What is the size of $\mathscr{P}_k$?

Denote $p_k = |\mathscr{P}_k|$ and we have for $4 \le k \le 58$ that

$p_4 = 2$, $p_5 = 2$, $p_6 = 5$, $p_7 = 4$, $p_8 = 5$, $p_9 = 7$, $p_{10} = 8$, $p_{11} = 8$, $p_{12} = 15$, $p_{13} = 14$, $p_{14} = 20$, $p_{15} = 34$, $p_{16} = 24$, $p_{17} = 34$, $p_{18} = 31$, $p_{19} = 54$, $p_{20} = 58$, $p_{21} = 93$, $p_{22} = 59$, $p_{23} = 78$, $p_{24} = 89$, $p_{25} = 123$, $p_{26} = 111$, $p_{27} = 185$, $p_{28} = 149$, $p_{29} = 182$, $p_{30} = 134$, $p_{31} = 257$, $p_{32} = 273$, $p_{33} = 384$, $p_{34} = 331$, $p_{35} = 498$, $p_{36} = 308$, $p_{37} = 471$, $p_{38} = 565$, $p_{39} = 663$, $p_{40} = 562$, $p_{41} = 674$, $p_{42} = 489$, $p_{43} = 840$, $p_{44} = 978$, $p_{45} = 1287$, $p_{46} = 866$, $p_{47} = 1184$, $p_{48} = 956$, $p_{49} = 1509$, $p_{50} = 1299$, $p_{51} = 1766$, $p_{52} = 1520$, $p_{53} = 1750$, $p_{54} = 1485$, $p_{55} = 2585$, $p_{56} = 2163$, $p_{57} = 2883$, $p_{58} = 2218$.

2. Nonabelian Φ

Theorem 13 ([2]). *If (N, Φ) is a circular Ferrero pair with Φ finite, then all Sylow subgroups of Φ are cyclic, i.e. Φ is metacyclic.*

The converse of the theorem is not true. There exists a Ferrero pair (N, Φ) with metacyclic Φ and (N, Φ) is not circular.

Theorem 14 ([2]). *Let (N, Φ) be a circular Ferrero pair with finite Φ. Then there is a nonempty finite subset $\mathscr{P}_{\Phi}$ of prime numbers with the following property: Let M be a finite group such that (M, Φ) is a Ferrero pair. Then (M, Φ) is circular if and only if $p \in {}_{\Phi}$ for all prime $p \mid |M|$.*

Remark. The assumption that (N, Φ) is circular Ferrero pair is used to guarantee the finiteness of $\mathscr{P}_{\Phi}$.

Thus, we said that a given group Φ

- is a *group without fixed points* if there is a group N such that (N, Φ) is a Ferrero pair, and
- a *circular group without fixed points* if there is a group M such that (M, Φ) is a circular Ferrero pair.

We have just seen that if Φ is a finite group without fixed points and Φ is circular, then Φ is metacyclic. But *not all metacyclic groups are circular*.

Question. Let Φ be finite metacyclic group (then Φ is a group without fixed points). Under what conditions is Φ circular?

(Zassenhaus 1936) Let Φ be a metacyclic group. Then $\Phi \cong \langle A, B \mid A^m = B^n = 1,\ B^{-1}AB = A^r \rangle$, where $m > 0$, $\gcd(m, (r-1)n) = 1$ and $r^n \equiv 1 \pmod{m}$. If d is the order of r modulo m, then all irreducible complex representation of Φ are of degree d.

Theorem 15 ([4]). *If $d = 2$ and if Φ is embeddable as a subgroup of the multiplicative group of some skew field K, then Φ is circular.*

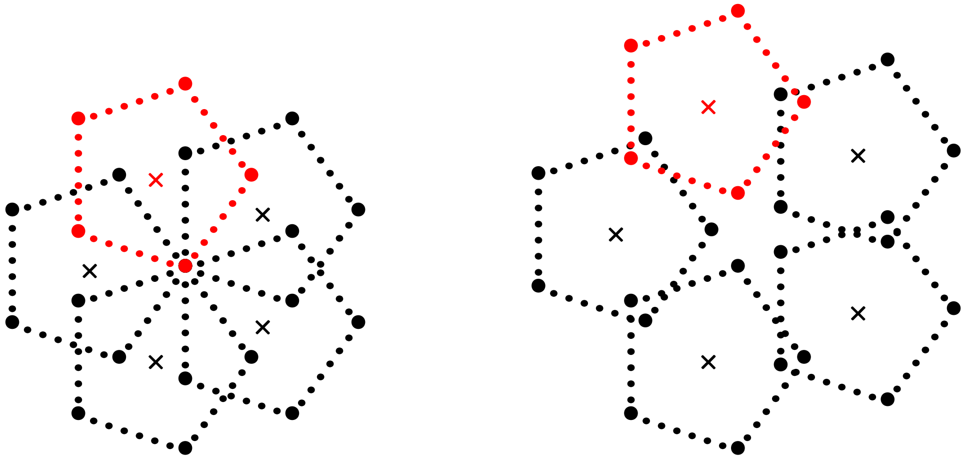
Conjecture. If Φ is a metacyclic group embeddable as a subgroup of the multiplicative group of some skew field K, then Φ is circular.

- Graphs

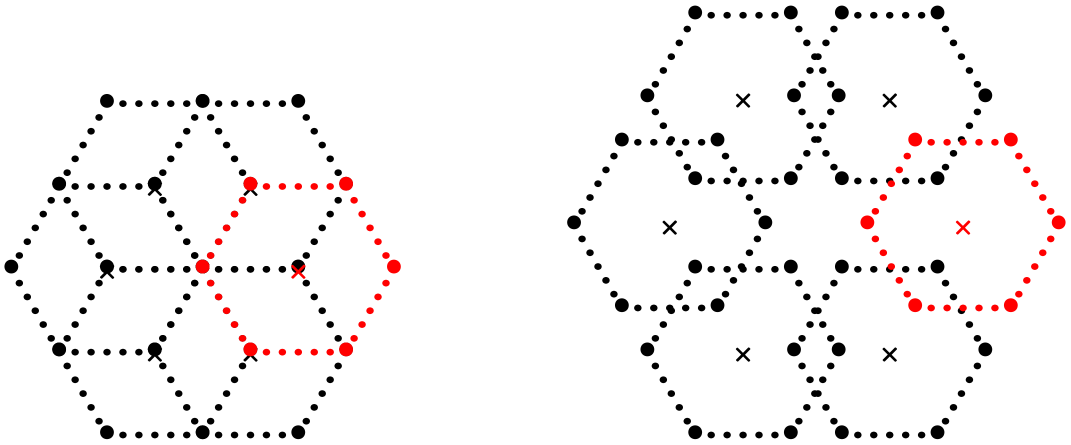
Let (N, Φ) be a Ferrero pair with finite Φ. For $r, c \in N \setminus \{0\}$, define

$$E_c^r = \{\Phi r + b \mid b \in \Phi c\}.$$

Example. (1) Two E_c^r's in $(\mathbb{C}, \Phi_5)$:$\Gamma_1^5 \vee \Gamma_2^5$:



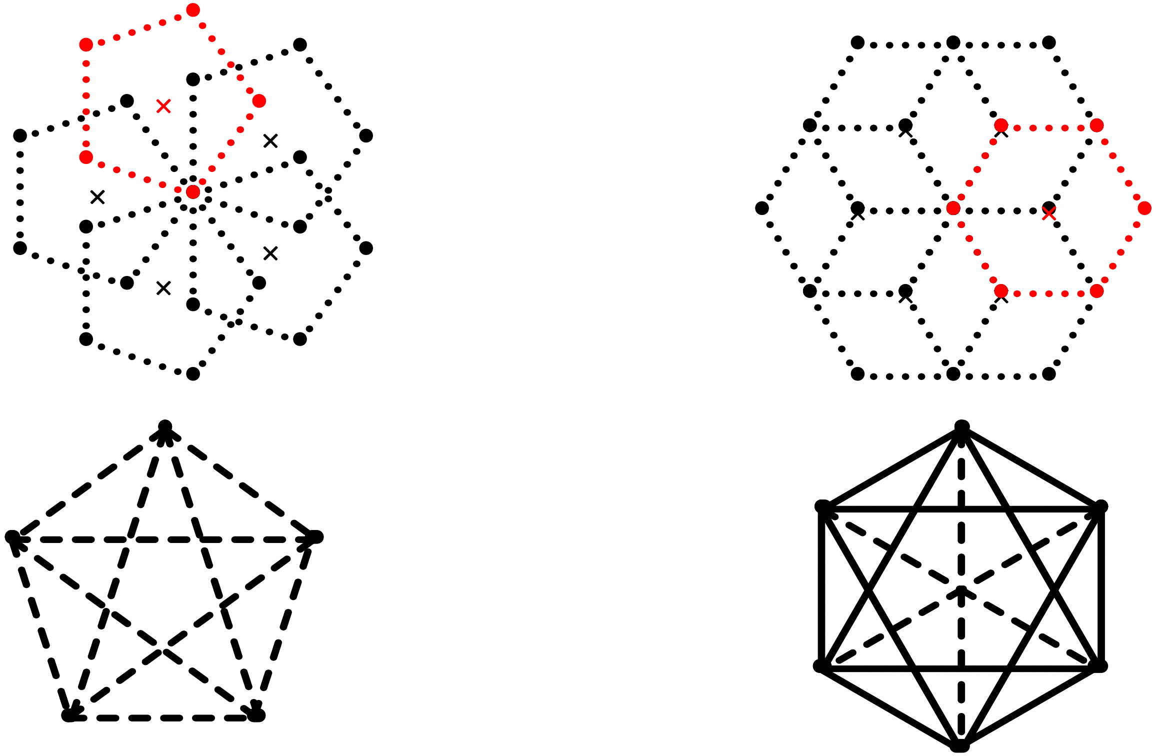
(2) Tow $\boldsymbol{E_c^r}$'s in $(\mathbb{C}, \boldsymbol{\Phi_6})$:



Assign to each $\boldsymbol{E_c^r}$ a graph $\boldsymbol{G(E_c^r)} = (\mathscr{V}, \mathscr{E})$: the vertex set $\mathscr{V} = \boldsymbol{\Phi c}$ and the edge set $\mathscr{E}$ is

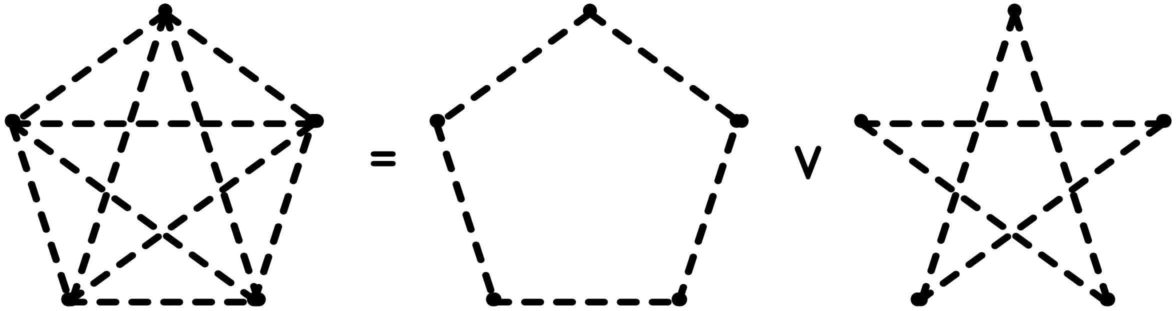
$\{\boldsymbol{c_1 c_2} \mid \boldsymbol{c_1}, \boldsymbol{c_2} \in \boldsymbol{\Phi c}, \boldsymbol{c_1} \neq \boldsymbol{c_2},$ and $(\boldsymbol{\Phi r}+\boldsymbol{c_1}) \cap (\boldsymbol{\Phi r}+\boldsymbol{c_2}) \neq \varnothing\}$.

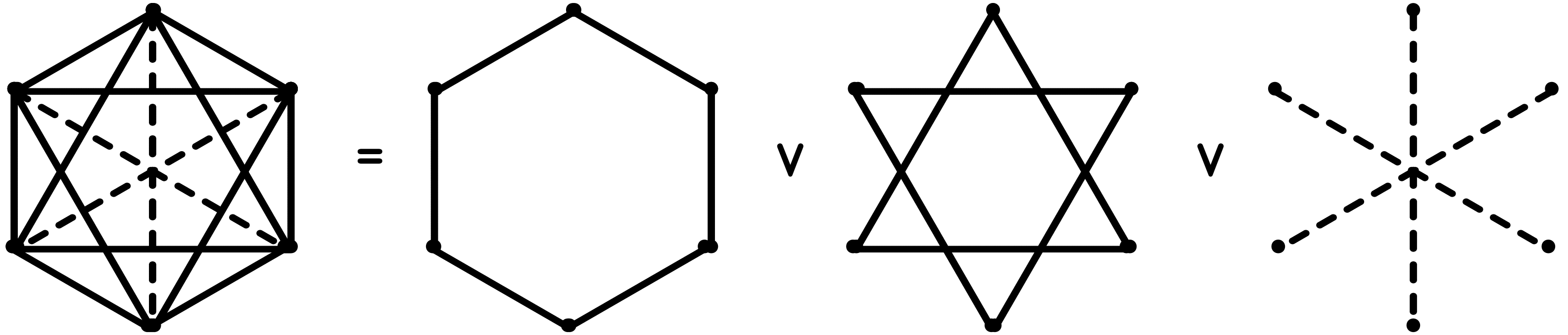
An edge $\boldsymbol{c}_1\boldsymbol{c}_2$ is *even* if $|(\Phi \boldsymbol{r} + \boldsymbol{c}_1) \cap (\Phi \boldsymbol{r} + \boldsymbol{c}_2)| = 2$, and is *odd* if $|(\Phi \boldsymbol{r} + \boldsymbol{c}_1) \cap (\Phi \boldsymbol{r} + \boldsymbol{c}_2)| = 1$.



- Every $\boldsymbol{G(E_c^r)}$ is a regular graph, i.e. all the vertices have the same number of edges connected to them.
- If $\boldsymbol{G(E_c^r)}$ has nonnull edges, then it is a union even and/or odd *basic graphs*.

Example.





1. Counting of basic graphs

   Suppose that N is a ring with unity and Φ a finite cyclic subgroup of the group of units of N such that (N, Φ) is a Ferrero pair (elements of Φ acts on N via left multiplication). (Such Ferrero pairs are said to be *ring generated*.) Let $|\Phi| = k$.

   Fix an $r \in N \setminus \{0\}$ and consider all $G(E_c^r)$, where $c \in N$, such that $G(E_c^r)$ has some edges. Then each of such graphs is either a basic graph or a "union" of basic graphs. Let γ_j denote the total number of appearance the odd j-th basic graphs in these nonnull graphs, and π_j the total number of appearance of the even j-th basic graphs.

Theorem 16 ([12]). *If* $2 \mid k$, *then* $\gamma_j = 1$ *and* $\pi_j = k/2 - 1$ *for any* $j \in \{1, 2, \ldots, k-1\}$.

Remark. The situation when Φ is nonabelian is also understood.

2. An application to solutions of equations.

Let $F = \mathrm{GF}(q)$ be the Galois field of order q. Let $k \mid (q-1)$ be such that (F, Φ_k) is a circular Ferrero pair.

Put $m = (q-1)/k$.

Denote by n the number of solutions of the equation

$$x^m + y^m - z^m = 1$$

in F, and by n' the number of solutions with $xyz \neq 0$.

Theorem 17 ([11]).

(1) *If k is even, then*

$$n = \begin{cases} 3(k-1)m^3 + 6m^2 + 3m & \text{if } 6 \mid k; \\ 3(k-1)m^3 + 3m^2 + 3m & \text{if } p = 3; \\ 3(k-1)m^3 + 3m & \text{otherwise;} \end{cases}$$

and $n' = 3(k-1)m^3$.

(2) *If k is odd, and if* $(\mathrm{GF}(q), \Phi_{2k})$ *is also circular, then*

$$n = (2k-1)m^3 + 2m \text{ and } n' = (2k-1)m^3.$$

3. Number of graphs in the complex plane case. Overlap problem.

   When (N, Φ) is a ring generated Ferrero pair with cyclic Φ, we observe that some of the basic graphs always appear together in some $G(E_c^r)$. A complete understanding of such behavior is the key to count the total number of graphs $G(E_c^r)$. Using a theorem of *vanishing sums* [Conway and Jones 1976, Theorem 6], we have a complete description of this phenomenon in the case of $(\mathbb{C}, \Phi_k)$, $\Phi_k \leq \widehat{C}$.

4. Asymptotic behavior.

So, we have noticed that basic graphs occur in the ring generated case are “fixed.” What makes finite field case and the complex plane case different is the overlaps of the basic graphs. Since the overlaps of the basic graphs are in one-one correspondence with the solutions (u, v, s, t) of the equations

$$\frac{\xi^u - 1}{\xi^v - 1} = \xi^w \frac{\xi^s - 1}{\xi^t - 1}$$

where ξ is a primitive k-th root of unity, $1 \le u < v \le s \le k-1$, $1 \le t \le k - 1$, $v \neq t$, $s \neq t$, and $1 \le w \le k - 1$.

Consider $\boldsymbol{\xi} = \boldsymbol{e}^{2\pi i/k} \in \mathbb{C}$ as before, and put the set $\mathscr{O}\mathscr{P}_{\boldsymbol{k}}$ the prime factors of the norms of

$$(\xi^{u} - 1)(\xi^{t} - 1) - \xi^{w}(\xi^{s} - 1)(\xi^{v} - 1)$$

for all possible $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{w}$. Then each $\mathscr{O}\mathscr{P}_{\boldsymbol{k}}$ is a finite set, and when $\boldsymbol{p}$ is a prime larger than any of that in $\mathscr{O}\mathscr{P}_{\boldsymbol{k}}$, the overlaps of the graphs of the $\boldsymbol{E}_{\boldsymbol{c}}^{\boldsymbol{r}}$'s from $(\mathrm{GF}(\boldsymbol{p}^{\boldsymbol{s}}), \boldsymbol{\Phi}_{\boldsymbol{k}})$ and $(\mathbb{C}, \boldsymbol{\Phi}_{\boldsymbol{k}})$ are the same.

Questions. An $\boldsymbol{E}_{\boldsymbol{c}}^{\boldsymbol{r}}$ is simply an equivalence class of a block $\boldsymbol{\Phi}_{\boldsymbol{k}}\boldsymbol{r} + \boldsymbol{b}$. Are there any other equivalence which will give use interesting (and hopefully manageable) equivalence classes?

What can we do with planar nearrings

A Group Discussion—10.07.2002 in JKU, Linz

An international research project

of Near-Linzers and Near-Tainaness

(1) The complex number field $\mathbb{C}$.

- ✔ How to distinguish the planar nearrings defined on $(\mathbb{C}, +)$?
- What to study in each individual planar?
- Characterize all fixed point free automorphism groups Φ on $(\mathbb{C}, +)$: $\Phi \leq (\mathbb{C}^*, \cdot)$, others, $\mathbb{C}$ as a $\mathbb{R}^2$, $\mathbb{C}$ as a vector space over $\mathbb{Q}$. Note that the descriptions of finite Φ's can be found in Wolf's book, "Spaces of constant curvature."

- Is being algebraically closed important for the study? How continuity may come into play?
- Any other constructions similar to Jim Clay's hyperbolas?

(2) The real number field $\mathbb{R}$ and $\mathbb{Q}$.

- The same questions as for $\mathbb{C}$.
- What else do we lose? Or do we really lose circles?

(3) ✓ Find field generated constructions other than the ones we have already known ($\mathbf{B}^*$, $\mathbf{B}^-$, $\mathbf{B}_0$, segments, lines, $\boldsymbol{S} \subseteq \boldsymbol{\Phi}$ [Buratti]). Do we get constructions which is different (and better, maybe) from those that combinatorics people have been using?

(4) Make possible visualization of planar nearrings.

(5) What can one do more about the triangle constructions of Jim Clay?

(6) Any connection of circles in circular planar nearrings with ovals in finite geometry?

(7) Make a dictionary among difference topics:

- Frobenius groups (1 affine complete; e.g. if $\boldsymbol{\Phi} = \mathbb{Z}_2$ on cyclic group of odd order; what are the ingredients to describe $\boldsymbol{\Phi}$? E.g. Is it true that $\boldsymbol{\Phi}$ must be $\mathbf{1}$-affine complete, or both $\boldsymbol{\Phi}$ and the kernel have to be $\mathbf{1}$-affine complete? Some case-by-case study? How about in $\mathbb{C}$?)
- Planar nearrings
- Design theory
- Difference families (sets)

Can one use the techniques or results in one area to apply to the others? E.g. building nearring structures (e.g. ideals, radicals) in the process of constructing planar nearrings from Ferrero pairs using the choices of subgroups for building ***A*** and the right units.

(8) Structure of planar nearrings

- ✓ What we have known: (left) ideals, radicals, IFP ⇒ integral.
- Generators (of planar nearrings, or modules)?
- Next? Tame? Planar nearring modules (can we describe them?)

(9) ✓ Representations of planar nearrings—nearring of functions on what modules?

(10) What is the variety generated by all planar nearrings, or all circular planar nearrings?

(11) ✓ The graphs of $\boldsymbol{E_c^r}$'s. Are they Cayley graphs? (They are subgraphs of Cayley graphs!)

Some open problems related to planar near-rings

Group Discussions - Linz - 07.08.2003

Problems suggested by Tim Boykett:

1. **Loop nearrings.** Using ideas similar to Silvia Pianta's, are there ways of using loop nearrings, or more generally, difference families on loops (or quasigroups), to generate designs? Quick results suggest that with a simple requirement, the definition of a difference family in quasigroups could make sense. Problems:

   - find some quasigroups that are not loops that are difference families

- find some quasigroups that allow a Ferrero pair type construction
- if these exist, then see whether at least some of the constructions can be generalised.

2. **Sub Difference Families.** It is often the case in the DFs constructed from Ferrero pairs using the ***B**** construction that there are several sub DFs. That is, subsets of the base blocks that form a DF, but with smaller λ. Thus the parameters that we obtain are not the only possible useful results. Comment from Ke at Hamburg emphasises that smaller λ values are of

interest. Thus these might be important. Problems:

- check subDFs for small examples
- collect any small results (there are some nonexistence results)
- what connections between subDF structure and Ferrero pair structure exist?
- are we obtaining new parameters?

3. **Generation.** What are the subnearrings generated by one element of a planar nearring? By two elements? How general can the generated nearrings be, when are they planar, when do we obtain the whole original nearring? These questions

arose (for me) from a series of thoughts about when the syntactic nearring of a group automaton would be planar.

4. **Visualisation.** Are there any nice visualisation techniques? Can we make any pretty pictures from these structures? Possible connection between the plane of the complex numbers and the graphs of the designs, relating to finite groups and their designs: e.g. the prime fields' graphs converge (in some well–defined sense) to the complex plane graphs. Getting some nice pictures (See "Not Knot" from the Geometry Center) http://www.geom.uiuc.edu/video/NotKnot/ is always a bit sexy and sort of useless.

Problems suggested by Weng-Fong Ke:

1. **Topological planar nearrings**

   (a) The complex plane case: Classify the topological planar nearrings generated by Ferrero pairs $(\mathbb{C}, \Phi)$ where Φ is a subgroup of the multiplicative group of $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

   (b) In general, it may be useful to use centralizer sandwich nearrings for studying topological planar nearrings.

2. **Designs:** Compare the designs which are planar nearring generated and the designs that have been studied in combinatorial design theory.

(a) Are there designs in the combinatorial design theory which can also be obtained using planar nearrings?

(b) Are there designs from planar nearrings which have not been studied in combinatorial design theory?

3. **Nonisomorphic planar nearrings.**

(a) Take small (N, Φ), compute $\mathscr{N}_{Aut(N)}(\Phi)$ and compare nonisomorphic planar nearrings to find properties that make the individual planar nearrings unique.

Note. There is a complete characterization of (N, Φ) with abelian N. (See *Frobenius groups and classical maximal orders* by Ron Brown, Memoirs 717; or *Characterization of* *some finite Ferrero pairs* by Ke and Kiechle, Fredericton Near-rings and near-fields Proceedigns, for elementary abelian and cyclic N with cyclic Φ).

4. **Matrix nearrings of planar nearrings.**

(a) Does the matrix nearring $M_n(N)$, where $N = (\mathbb{C}, +, *_E)$, have nice properties (eg. behave like a generalization of n dimensional vector spaces)?

(b) In general, study matrix nearrings of planar nearrings. Do they possess good properties?

Problems suggested by Peter Mayr:

1. **Varieties.** Which varieties generated by the following classes of near-rings are equal and which are distinct?

   A ... class of finite near-fields,

   B ... class of zero-symmetric near-rings with abelian additive group,

   C ... class of finite integral planar near-rings,

   D ... class of finite zero-symmetric integral near-rings,

   E ... class of finite zero-symmetric near-rings satisfying $\boldsymbol{x^n = x}$ for some natural number $\boldsymbol{n}$,

   F ... class of zero-symmetric near-rings.

Note that D $\subseteq$ E, and that the subdirectly irreducible elements of E are in D. Thus the varieties generated by $\mathbf{D}$ and by $\mathbf{E}$ are equal.

2. Related to the previous question: We know that the class of finite Frobenius kernels generates the variety of all groups, since each finite p-group can be embedded into a Frobenius kernel.

   (a) Does the class of Frobenius complements of Frobenius groups also generate the variety of all groups?

   (b) Determine the variety generated by the multiplicative semigroups of (finite) planar near-rings.

3. **Near-fields.** Is there an infinite near-field whose multiplicative group has finite exponent? (There is none with exponent $\mathbf{3, 6, 12}$, or $\mathbf{2}^{\boldsymbol{n}}$ for any natural number $\boldsymbol{n}$.)

Problems suggested by Gerhard Wendt:

1. **Regularity.** Study the connection between 2-primitive near-rings and regularity. Regularity of elements (defined in the usual sense for semigroups) seem to play a very vital role in the structure of 2-primitive ner-rings. For example, every minimal left ideal of a 2-primitive near-ring is planar and hence “very” regular, in particular, the regular elements form a (multiplicative) subsemigroup there. Does the same hold for a 2-primitive near-ring, do the regular elements form a subsemigroup? It seems to be the case that 2-primitive near-rings with identity (which basically are centralizer near-rings of

the form $M_G(\Gamma)$, G fixedpointfree on Γ) are regular near-rings. This also has not been worked out yet properly.

2. Referring to the first item, if there can be said something about 2-primitive near-rings then it should also be possible to get results on 2-semisimple near-rings.

3. **Planar subnear-rings.** Planar substructures or at least planar like structures arise naturally in 2- and 1-primitive near-rings. What about 0-primitive near-rings or near-rings which may be seen very primitive like (e.g put conditions on near-ring modules).

4. **K-loops.** Is there something to say about possible connections between K-loops and planar near-rings? Do techniques for studying planar near-rings carry over to K-loops.

5. **Planar quotients.** If one needs still a problem, study quotients of near-rings and determine when they are planar.

References

[1] M. Anshel and J. R. Clay. Planar algebraic systems: some geometric interpretations. *J. Algebra* **10** (1968), 166–173.

[2] K. I. Beidar, Y. Fong, and W.-F. Ke. On finite circular planar nearrings. *J. Algebra* **185** (1996), 688–709.

[3] K. I. Beidar, Y. Fong, and W.-F. Ke. Maximal right nearring of quotients and semigroup generalized polynomial identity. *Result. Math.* **42** (2002), 12–27.

[4] K. I. Beidar, W.-F. Ke, and H. Kiechle. Circularity of finite groups without fixed points. 1999, submitted.

[5] K. I. Beidar, W.-F. Ke, and H. Kiechle. Automorphisms of design groups II. 2003, submitted.

[6] K. I. Beidar, W.-F. Ke, C.-H. Liu, and W.-R. Wu.

Automorphism groups of certain simple $\mathtt{2}$-$(q, 3, \lambda)$ designs constructed from finite fields. *Finite Fields Appl*, to appear.

[7] J. R. Clay. Circular block designs from planar nearrings. *Ann. Discrete Math.* **37** (1988), 95–106.

[8] J. R. Clay. Geometry in fields. *Algebra Colloq.* **1** (1994), 289–306.

[9] G. Ferrero. Stems planari e bib-disegni. *Riv. Mat. Univ. Parma (2)* **11** (1970), 79–96.

[10] W. F. Ke and H. Kiechle. Automorphisms of certain design groups. *J. Algebra* **167** (1994), 488–500.

[11] W. F. Ke and H. Kiechle. On the solutions of the equation $x^m + y^m - z^m = 1$ in a finite field. *Proc. Amer. Math. Soc.* **123** (1995), 1331–1339.

[12] W.-F. Ke and H. Kiechle. Combinatorial properties of ring generated circular planar nearrings. *J. Combin. Theory Ser. A* **73** (1996), 286–301.

[13] M. C. Modisett. *A characterization of the circularity of certain balanced incomplete block designs*. Ph. D. dissertation, University of Arizona, 1988.

[14] M. Modisett. A characterization of the circularity of balanced

incomplete block designs. *Utilitas Math.* **35** (1989), 83–94.

[15] H.-M. Sun. Segments in a planar nearring. *Discrete Math.* **240** (2001), 205–217.

[16] H.-M. Sun. PBIB designs and association schemes obtained from finite rings. *Discrete Math.* **252** (2002), 267–277.

[17] G. Wendt. A description of all planar near-rings. Preprint.

[18] G. Wendt. Planar near-rings and sandwich near-rings. Preprint.