Mathematisches Seminar

Hamburger Beiträge zur Mathematik
Heft 248

Automorphisms of Certain Design Groups II

Kostia I. Beidar, Wen-Fong Ke,
Hubert Kiechle

Universität Hamburg

AUTOMORPHISMS OF CERTAIN DESIGN GROUPS II

KOSTIA I. BEIDAR, WEN-FONG KE[1], HUBERT KIECHLE[2]

Abstract. Let Φ be a group acting fixed point freely as automorphisms on the group $(N,+)$. This gives rise to a certain 2-design $(N,\mathbf{B}_\Phi)$. The group structure of N is compatible with the geometric structure of this 2-design, and we call $(N,\mathbf{B}_\Phi,+)$ a *design group.*

Extending our previous results, we study the question when such design groups are isomorphic. Let Ψ be another group acting on N so that $(N,\mathbf{B}_\Psi,+)$ is also a design group. Suppose further that for $k=|\Phi|$ we have $|N/[N,N]|>2k^2-6k+1$. We show that $(N,\mathbf{B}_\Phi,+)$ and $(N,\mathbf{B}_\Psi,+)$ are isomorphic if and only if Φ and Ψ are conjugate in the automorphism group of N.

Introduction

Let $(N,+)$ be a not necessarily abelian, finite group. Let Φ be a subgroup of $\operatorname{Aut} N$ acting fixed point freely on N. This means that for $\varphi\in\Phi$ we have $\varphi=\mathrm{id}$ or $\varphi(x)=x$ implies that $x=0$. Then (N,Φ) will be called a *Ferrero pair.* Notice that the semidirect product $N\rtimes\Phi$ is a Frobenius group. Conversely, every Frobenius group gives rise to a Ferrero pair by taking the kernel as N and a one point stabilizer as Φ.

Define $\mathbf{B}_\Phi=\{\Phi a+b\mid a,b\in N, a\neq 0\}$, where each $\Phi a+b=\{\varphi(a)+b\mid\varphi\in\Phi\}$ is the shifting of the orbit Φa of a by b. Then $(N,\mathbf{B}_\Phi)$ is a 2-design (cf. [4, (5.5)]). Since N acts by right translation as an automorphism group on this design, we call $(N,\mathbf{B}_\Phi,+)$ a *design group.*

An isomorphism of design groups is a an isomorphism of the group structure which preserves also the design structure. In [8, (3.2)] and [8, (3.3)] we proved the following theorem.

The first author passed away before this paper was complete.

[1] Partially supported by National Science Council, R.O.C..

[2] Partially supported by DAAD.

Theorem 1. *Let (M,Ψ) and (N,Φ) be finite Ferrero pairs with M, N, Φ, and Ψ abelian, and let f be an isomorphism from $(M, \mathbf{B}_\Psi, +)$ to $(N, \mathbf{B}_\Phi, +)$. Put $k = |\Phi|$. If $|N| > k+1$, then $f\Psi f^{-1} = \Phi$. In particular, if $(M,\Psi) = (N,\Phi)$, then f is a normalizer of Φ in* $\mathrm{Aut}N$.

Remark. 1. The condition $f\Psi f^{-1} = \Phi$ means that the permutation actions of Ψ on M and of Φ on N are equivalent. Therefore such an f will also be called an *equivalence* of the Ferrero pairs. In this case the involved Ferrero pairs are said to be *equivalent*.

2. The statement of [8, (3.2)] is not quite correct. There the hypothesis $|N| > k+1$ is missing. Indeed, if $|N| = k+1$, then every permutation of N is an automorphism of the design. Thus there exist examples of design group isomorphisms which are not equivalences. However, the proof of [8, (3.2)] does show Theorem 1 as it is stated here.
3. Here's the smallest counterexample: Let N be the field of 8 Elements and $\Phi = N^*$. Then (N,Φ) is a Ferrero pair. The (simple!) group $\mathrm{GL}(3,2)$ of order 168 acts on $(N,+)$ as automorphism group, hence on the design as design group automorphisms. However, it certainly does not normalize Φ. (The normalizer of Φ has 21 elements.)

The aim of the present article is to consider the case when M, N, Φ, and Ψ may be nonabelian. That is, we will prove the following theorem.

Main Theorem. *Let (M,Ψ) and (N,Φ) be finite Ferrero pairs and let f be an isomorphism from $(M, \mathbf{B}_\Psi, +)$ to $(N, \mathbf{B}_\Phi, +)$. Put $k = |\Phi|$. If $|N/[N,N]| > 2k^2 - 6k + 1$, then $f\Psi f^{-1} = \Phi$, i.e., f is an equivalence of the involved Ferrero pairs.*

Corollary. *Let (N,Φ) be a finite Ferrero pair with $k = |\Phi|$. If $|N/[N,N]| > 2k^2 - 6k + 1$, then $Aut(N, \mathbf{B}_\Phi, +)$ is the normalizer of Φ inside $Aut(N,+)$.*

Notice that due to the bound for $|N/[N,N]|$, Main Theorem does not imply Theorem 1. Because in the abelian case the Theorem 1 gives a much better bound except for $k = 3$. However, the case $k = 3$ complicates the proof of Main Theorem.

After the preliminary section, Sections 2, 3 and 4 are devoted to prove the Main Theorem. In Section 2, we consider the condition $f(\Phi(a)) = \Phi f(a)$ for all $a \in N$. In Section 3, we work out the case $k = 3$. Then in Section 4, we prove a crucial result which leads to the proof of Main Theorem. Finally, in the Sections 5 and 6 we discuss the bound, and show by examples that some bound is necessary. The quality of the bound is also discussed.

1. Ferrero pairs

Take a Ferrero pair (N, Φ) with finite N and nontrivial Φ. Customarily, we set $v = |N|$ and $k = |\Phi|$. For any subset M of an additively written group, let $M^* = M \setminus \{0\}$. Then it holds that

(N1) $k \,\big|\, (v-1)$ [7, Theorem 10.3.1];
(N2) N is nilpotent [7, Theorem 10.2.1];
(N3) $\{\Phi\, a \mid a \in N^*\}$ is a partition of N^* with $|\Phi\, a| = |\Phi| = k$ for all $a \in N^*$.

For any automorphism $f : N \to N$ and any invariant normal subgroup V of N, there are two induced maps $f|_V$ and $\widehat{f}$ that come into play. The mapping $f|_V$ is simply the restriction of f to V, while the mapping $\widehat{f} : N/V \to N/V$ is given by $\widehat{f}(a+V) = f(a) + V$ for all $a \in N$. We'll use $\overline{x}$ for $x + V \in N/V$ if V is clear from the context. Thus, we have $\widehat{f}(\overline{a}) = \overline{f(a)}$.

Let α be a fixed point free automorphism of N. Then $\alpha|_V$ and $\widehat{\alpha}$ are fixed point free automorphisms of V and N/V, respectively (cf. [7]).

We remark that the nonzero orbits of Φ form a $(v, k, k-1)$-*difference family*. The development of this difference family is just $(N, \mathbf{B}_\Phi)$. The automorphisms of the design group $(N, \mathbf{B}_\Phi, +)$ are also called *(right) multipliers* of the difference family. See [2] for more details.

2. First Step

Throughout the rest of the paper, (M, Ψ) and (N, Φ) are finite Ferrero pairs, and f is an isomorphism of the design groups $(M, \mathbf{B}_\Psi, +)$ and $(N, \mathbf{B}_\Phi, +)$. Also, we recall that $v = |N|$ and $k = |\Phi|$.

If $(N, +)$ is abelian, it was shown that f preserves the orbits (the base blocks of the designs), i.e. $f(\Psi a) = \Phi f(a)$ for all $a \in M$ [8, (1.5)]. If Φ is also abelian and $v > k + 1$, then Theorem 1 shows that f normalizes Φ.

Remark 2.1. We notice that preserving the base blocks is a strong condition.

Assume that $f(\Phi a) = \Phi f(a)$ for all $a \in N$ and let $\varphi \in \Phi$. Then for each $x \in N^*$, there is a unique $\lambda_x \in \Phi$ depending on x such that

$$f(\varphi(x)) = \lambda_x(f(x)).$$

Assume further that f normalizes Φ. Then $f\varphi f^{-1} \in \Phi$, and

$$\lambda_x(f(x)) = f(\varphi(x)) = (f\varphi f^{-1})(f(x)).$$

Since $f(x) \neq 0$, and $\lambda_x, f\varphi f^{-1} \in \Phi$ are fixed point free, it follows that $\lambda_x = f\varphi f^{-1}$. Therefore, λ_x is *independent* of x.

In the following theorem, we show that under some "separation condition," the orbits preserving condition leads to the normalizing condition.

Theorem 2.2. *Let (M, Ψ) and (N, Φ) be finite Ferrero pairs, and let f be an isomorphism of the design groups $(M, \mathbf{B}_\Psi, +)$ and $(N, \mathbf{B}_\Phi, +)$. Suppose that for any $s, t \in N^*$, there is an element $z \in N^*$ (depending on s and t) such that*

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-z) + z\big) = \big(\Phi(-t) + t\big) \cap \big(\Phi(-z) + z\big) = \{0\}. \tag{2.1}$$

If $f(\Psi x) = \Phi f(x)$ for all $x \in M$, then $f\Psi f^{-1} = \Phi$.

Proof. Let $\psi \in \Psi$. For $x \in M^*$, we can find $\lambda_x \in \Phi$ such that $f(\psi(x)) = \lambda_x(f(x))$. With Remark 2.1 in mind, we set the course to show that $\lambda_x = f\psi f^{-1}$, hence it does not depend on x. Then it would readily follow that $f\Psi f^{-1} = \Phi$.

Take arbitrary $x, y \in M^*$. We have, on one hand,

$$f(\psi(x-y)) = \lambda_{x-y}(f(x-y)) = \lambda_{x-y}(f(x)) - \lambda_{x-y}(f(y));$$

and on the other,

$$f(\psi(x-y)) = f(\psi(x)) - f(\psi(y)) = \lambda_x(f(x)) - \lambda_y(f(y)).$$

Therefore,

$$\lambda_x(f(x)) - \lambda_y(f(y)) = \lambda_{x-y}(f(x)) - \lambda_{x-y}(f(y)),$$

or equivalently,

$$\begin{aligned}\lambda_x(-f(x)) + \lambda_{x-y}(f(x)) &= -\lambda_x(f(x)) + \lambda_{x-y}(f(x)) \\ &= -\lambda_y(f(y)) + \lambda_{x-y}(f(y)) = \lambda_y(-f(y)) + \lambda_{x-y}(f(y)).\end{aligned}$$

This yields

$$(\lambda_{x-y}^{-1}\lambda_x)(-f(x)) + f(x) = (\lambda_{x-y}^{-1}\lambda_y)(-f(y)) + f(y),$$

which is an element of $\big(\Phi(-f(x)) + f(x)\big) \cap \big(\Phi(-f(y)) + f(y)\big)$. Thus, if

$$\big(\Phi(-f(x)) + f(x)\big) \cap \big(\Phi(-f(y)) + f(y)\big) = \{0\},$$

then $\lambda_x = \lambda_{x-y} = \lambda_y$.

Now using the fact that f is an isomorphism and (2.1), we see that for any $a, b \in M^*$, there is an element $c \in M^*$ such that

$$\big(\Phi(-f(a)) + f(a)\big) \cap \big(\Phi(-f(c)) + f(c)\big) = \{0\}$$

and

$$\big(\Phi(-f(b)) + f(b)\big) \cap \big(\Phi(-f(c)) + f(c)\big) = \{0\};$$

hence, $\lambda_a = \lambda_c = \lambda_b$. That is, we have

$$f(\psi(b)) = \lambda_b(f(b)) = \lambda_a(f(b)).$$

Since b is arbitrary, we have $f\psi = \lambda_a f$. Therefore, $f\psi f^{-1} = \lambda_a \in \Phi$. This completes the proof. □

Now we shall inspect the condition (2.1).

Lemma 2.3. *Assume $v > 2k^2 - 6k + 7$. Then for $s, t \in N^*$, there exists an element $z \in N^*$ such that*

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-z) + z\big) = \big(\Phi(-t) + t\big) \cap \big(\Phi(-z) + z\big) = \{0\}.$$

Proof. We put

$$\mathcal{A} = \{(-\varphi_1 + 1)^{-1}(-\varphi_2 + 1) \mid \varphi_1, \varphi_2 \in \Phi \setminus \{1\},\ \varphi_1 \neq \varphi_2\}.$$

For any $x \in N^*$, set $\mathcal{A}_x = \{\tau(x) \mid \tau \in \mathcal{A}\}$. It is clear that

$$|\mathcal{A}_x| \le |\mathcal{A}| \le (k-1)(k-2).$$

Take an $a \in N^* \setminus \{s\}$. If $w \in N^*$ such that

$$w \in \big(\Phi(-s) + s\big) \cap \big(\Phi(-a) + a\big).$$

Then

$$(-\varphi_1 + 1)(s) = \varphi_1(-s) + s = w = \varphi_2(-a) + a = (-\varphi_2 + 1)(a)$$

for some distinct $\varphi_1, \varphi_2 \in \Phi \setminus \{1\}$. Thus $a = (-\varphi_2 + 1)^{-1}(-\varphi_1 + 1)(s) \in \mathcal{A}_s$. Therefore, if

$$v > (k-1)(k-2) + 2 = k^2 - 3k + 4 \tag{2.2}$$

(counting 0 and s as well), then $N \setminus \big(\{0, s\} \cup \mathcal{A}_s\big) \neq \varnothing$. Hence we may pick some $y \in N \setminus \big(\{0, s\} \cup \mathcal{A}_s\big)$. This would give

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-y) + y\big) = \{0\}.$$

Similarly, if

$$v > 2(k-1)(k-2) + 3 = 2k^2 - 6k + 7,$$

then $N \setminus \big(\{0, s, t\} \cup \mathcal{A}_s \cup \mathcal{A}_t\big) \neq \varnothing$. Simply pick an arbitrary z from the set $N \setminus \big(\{0, s, t\} \cup \mathcal{A}_s \cup \mathcal{A}_t\big)$, and we would have

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-z) + z\big) = \big(\Phi(-t) + t\big) \cap \big(\Phi(-z) + z\big) = \{0\}.$$

This is what we wanted. □

3. Small $N/[N, N]$ with $k = 3$

Special consideration is needed for the case $k = 3$. Of course, Φ and Ψ are cyclic in this case. We shall freely use the fact that N is nilpotent.

First we remove the bound from Theorem 1 in this special case (cf. [1]).

Lemma 3.1. *Suppose that M and N are abelian and $k = 3$. Then $f\Psi f^{-1} = \Phi$.*

Proof. There is no loss in generality to assume $M = N$. If $|N| > 4$ then Theorem 1 applies to give the result.

Thus we are left with the case $N = \mathbb{Z}_2 \times \mathbb{Z}_2$. Now $\operatorname{Aut} N = \mathrm{GL}(2, 2)$ has 6 elements, so Φ is a normal subgroup of $\operatorname{Aut}(N, +)$ and the result follows. □

Let $Z_0 = \{0\} \leq Z_1 \leq \cdots \leq Z_{n-1} \lneqq Z_n = N$ be the upper central series of N. This is defined recursively by $Z_i := \{x \in N \mid \forall y \in N : [x, y] \in Z_{i-1}\}$. In this case, the nilpotency class of N is n. Note that Z_1 is the center of N. Also, let $N = N_0 \geq N_1 \geq \cdots \geq N_n = \{0\}$, be the lower central series of N. Again, this is given recursively by $N_1 = [N, N]$, and $N_i = [N_{i-1}, N]$ for $i = 1, 2, \ldots, n$. Recall that n is the same in both cases. So, N is of nilpotency class n if and only if $N_{n-1} \neq \{0\}$ and $N_{n-1} \subseteq Z_1$. (See [7, §2.3].)

Lemma 3.2. *Suppose that N is nonabelian and $k = 3$. Let $s, t \in N^*$ be such that*

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-t) + t\big) \neq \{0\}.$$

Then $s \in Z_i$ if and only if $t \in Z_i$ for every i.

Proof. Since Φ is cyclic, we may assume that it consists of 1, φ, and φ^2. By [7, Lemma 10.1.1], we have for all $x \in N$,

$$x + \varphi(x) + \varphi^2(x) = 0.$$

Since $(\varphi^2)^2 = \varphi$, we also have $x + \varphi^2(x) + \varphi(x) = 0$ for all $x \in N$. From these two, we conclude that for any $x \in N$, the elements x, $\varphi(x)$ and $\varphi^2(x)$ commute pairwise.

Take distinct $s, t \in N^*$. If $(\Phi(-s)+s)\cap(\Phi(-t)+t) \neq \{0\}$, then exactly one of the following cases holds: (1) $\varphi(-s)+s = \varphi(-t)+t$, (2) $\varphi^2(-s)+s = \varphi^2(-t)+t$, (3) $\varphi(-s)+s = \varphi^2(-t)+t$, and (4) $\varphi^2(-s)+s = \varphi(-t)+t$. In case (1), we have $\varphi(t-s) = t-s$, which is not possible as $\varphi \neq 1$ and $t \neq s$. Similarly, case (2) is not possible. Cases (3) and (4) are symmetric; thus it suffices to consider case (3). We have

$$\varphi(t) + 2t = \varphi^2(-t) + t = \varphi(-s) + s = \varphi^2(s) + 2s. \tag{3.1}$$

Applying φ to both ends of the last equations, we get

$$\varphi^2(t) + 2\varphi(t) = s + 2\varphi(s).$$

Now, $\varphi^2(t) + 2\varphi(t) = -t - \varphi(t) + 2\varphi(t) = -t + \varphi(t)$, and so

$$-t + \varphi(t) = s + 2\varphi(s).$$

Combining this equation with (3.1), we have

$$\begin{aligned} 3t &= (\varphi(t) + 2t) - (-t + \varphi(t)) \\ &= (\varphi(-s) + s) - (s - 2\varphi(s)) = -3\varphi(s). \end{aligned} \tag{3.2}$$

Assume s is from Z_i. Then (3.2) implies that

$$3(t + \varphi(s)) \equiv 0 \pmod{Z_{i-1}}.$$

Since $3 \,\big|\, (|N| - 1)$ by (N1), N cannot have elements of order 3. This implies that

$$t \equiv -\varphi(s) \pmod{Z_{i-1}},$$

and so $t \in Z_i$ as well. Similarly, if $t \in Z_i$, then $s \in Z_i$. The proof is complete. $\square$

Lemma 3.3. *Suppose that N is a nonabelian p-group, $k = 3$, and $|N/[N,N]| = 4$ or 7. Then for $s, t \in N^*$ there exists $u \in N$ such that*

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-u) + u\big) = \big(\Phi(-t) + t\big) \cap \big(\Phi(-u) + u\big) = \{0\}.$$

Proof. Let $\bar{v} = |N/[N,N]|$. We continue to use the upper central series of N defined just before Lemma 3.2. Let $i > 0$ and $j > 0$ be such that $s \in Z_i \setminus Z_{i-1}$ and $t \in Z_j \setminus Z_{j-1}$. If the nilpotency class n of N is greater than 2, then there exists $0 < k \leq n$ with $k \notin \{i, j\}$. By Lemma 3.2, any $u \in Z_k \setminus Z_{k-1}$ would do the job. The same argument works if $n = 2$ and $i = j$.

So we are left with the case $n = 2$. By symmetry we can assume that $s \in Z_1$ and $t \in N \setminus Z_1$. Since Φ acts fixed point freely on Z_1, we know that

$$|Z_1| \geq k + 1 = 4 = k^2 - 3k + 4.$$

Now, if $|Z_1| > 4$, then the proof of Lemma 2.3 (see (2.2) and the following lines) applies to the Ferrero pair (Z_1, Φ). Thus, there exists some $u \in Z_1$ such that

$$\big(\Phi(-s) + s\big) \cap \big(\Phi(-u) + u\big) = \{0\}.$$

Since $t \notin Z_1$, it follows from Lemma 3.2 that

$$\big(\Phi(-t) + t\big) \cap \big(\Phi(-u) + u\big) = \{0\},$$

and we are done.

So we are left with $\bar{v} = 4 = |Z_1|$. From $n = 2$ we have $[N, N] \subseteq Z_1$. Again, as $[N, N] \neq \{0\}$ and Φ acts fixed point freely on $[N, N]$, we have $|[N, N]| \geq 4$, and so $[N, N] = Z_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$. But inspecting the list of all groups N of order 16 using GAP [6] shows that there is no group satisfying all these conditions. □

4. Proof of Main Theorem

We now come to the crucial step of our proof.

Theorem 4.1. *Let (M, Ψ) and (N, Φ) be finite Ferrero pairs and let f be an isomorphism from $(M, \mathbf{B}_\Psi, +)$ to $(N, \mathbf{B}_\Phi, +)$. Put $k = |\Phi|$. If $k = 3$ or $|N/[N, N]| > 2k^2 - 6k + 7$, then $f \Psi f^{-1} = \Phi$.*

Proof. Here we will make use of the lower central series of N (see the paragraph before Lemma 3.2). Thus, $N_1 = [N, N]$, and $N_i = [N_{i-1}, N]$ for $i = 1, 2, \ldots, n$. Suppose that N is of nilpotency class n. Hence $\{0\} \neq N_{n-1} \subseteq Z_1$, the center of N. The proof will be proceed by induction on n.

Let $n = 1$, i.e. N is abelian. If $k = 3$, the result follows immediately from Lemma 3.1. If $k > 3$, then Lemma 2.3 together with [8, (1.5.2)] show the hypotheses of Theorem 2.2. Consequently, $f \Psi f^{-1} = \Phi$.

Now, let $n > 1$ be minimal such that f is an isomorphism of the design groups $(M, \mathbf{B}_\Psi, +)$ and $(N, \mathbf{B}_\Phi, +)$ yet $f \Psi f^{-1} \neq \Phi$. Note that, by Lemmas 2.3 and 3.3, and Theorem 2.2, we can find $s \in M^*$ and $a, b \in N^*$ such that

$$f(\Psi(s)) = \Phi(a) + b. \tag{4.1}$$

Also, as M and N are isomorphic groups, M is of nilpotency class n as well.

We set out to find a contradiction derived from (4.1).

Denote by $V = N_{n-1}$. Then N/V is of class $n-1$. Each nonidentity mapping $\varphi \in \Phi$ induces a fixed point free automorphism $\widehat{\varphi}$ of N/V via $\widehat{\varphi}(\overline{s}) = \overline{\varphi(s)}$, where $\overline{s} = s + V$, for all $s \in N$. Put $\widehat{\Phi} = \{\widehat{\varphi} \mid \varphi \in \Phi\}$. Then $(N/V, \widehat{\Phi})$ is a finite Ferrero pair. Similarly, let $U = M_{n-1}$ and $\widehat{\Psi} = \{\widehat{\psi} \mid \psi \in \Psi\}$, where $\widehat{\psi}(\overline{s}) = \widehat{\psi}(s + U) = \overline{\psi(s)} = \psi(s) + U$ for all $s \in M$ (using the $\overline{\cdot}$ notation for M/U as well). Then $f(U) = V$ and f induces an isomorphism $\widehat{f}$ from M/U to N/V via $\widehat{f}(\overline{s}) = \overline{f(s)}$ for all $\overline{s} \in M/U$. Moreover, $\widehat{f}$ is an isomorphism of the design groups $(M/U, \mathbf{B}_{\widehat{\Psi}}, +)$ and $(N/V, \mathbf{B}_{\widehat{\Phi}}, +)$. Indeed, suppose that $f(\psi(s) + t) = \varphi(a) + b$ where $s, t \in M$, $\psi \in \Psi$, $a, b \in N$, $\varphi \in \Phi$, and $\overline{s}$ and $\overline{a}$ are nonzero. Then

$$\widehat{f}(\widehat{\psi}(\overline{s}) + \overline{t}) = \widehat{f}(\overline{\psi(s) + t}) = \overline{f(\psi(s) + t)} = \overline{\varphi(a) + b} = \widehat{\varphi}(\overline{a}) + \overline{b} \in \widehat{\Phi}\overline{a} + \overline{b};$$

hence $\widehat{f}(\widehat{\Psi}(\overline{s}) + \overline{t}) = \widehat{\Phi}\overline{a} + \overline{b}$. Now, since $V \subseteq [N, N] = N_1$, we have

$$\begin{aligned} |(N/V)/[N/V, N/V]| &= |(N/V)/([N, N]/V)| \\ &= |N/[N, N]| > 2k^2 - 6k + 7. \end{aligned}$$

The minimality of n implies that $\widehat{f}\widehat{\Psi}\widehat{f}^{-1} = \widehat{\Phi}$. In particular,

$$\widehat{\Phi}\widehat{f}(\overline{x}) = \widehat{f}(\widehat{\Psi}(\overline{x})) \quad \text{for all } \overline{x} \in M/U. \tag{4.2}$$

Now for the element s in (4.1), there are two possibilities: either $s \in U$ or $s \notin U$. It is easy to rule out the first possibility. Indeed, since U and V are a characteristic subgroups or Ψ and Φ respectively, (U, Ψ) and (V, Φ) are also Ferrero pairs. It is clear that $f|_U$ is an isomorphism of the corresponding design groups from (U, Ψ) and (V, Φ). As U and V are abelian, $s \in U$ would yield $b = 0$ by [8, (1.5)], which is not in our consideration.

So we are left with the case $s \notin U$, or equivalently, $\overline{s} \neq \overline{0}$. In turn, this implies that $\overline{a} \neq \overline{0}$. By (4.2), we have

$$\widehat{\Phi}\widehat{f}(\overline{s}) = \widehat{f}(\widehat{\Psi}(\overline{s})) = \widehat{\Phi}\overline{a} + \overline{b}.$$

Hence $\overline{b} = \overline{0}$ and $\overline{a} = \widehat{\tau}(\widehat{f}(\overline{s}))$ for some $\tau \in \Phi$. Put $a' = \tau^{-1}(a)$. Then

$$\Phi a' = \Phi\tau^{-1}(a) = \Phi a$$

and

$$\widehat{\Phi}\overline{a'} = \widehat{\Phi}\widehat{\tau}^{-1}(\overline{a}) = \widehat{\Phi}\widehat{\tau}^{-1}(\widehat{\tau}\widehat{f}(\overline{s})) = \widehat{\Phi}\widehat{f}(\overline{s}).$$

Thus, replacing a by a' if necessary, we may assume that $\overline{a} = \widehat{f}(\overline{s})$. We note that $\overline{a'} \neq \overline{0}$ as well.

Let $\theta : \Psi \to \Phi$ be the bijection such that

$$f(\psi(s)) = \theta(\psi)(a) + b \quad \text{for all } \psi \in \Psi.$$

Pick an arbitrary $\sigma \in \Psi \setminus \{1\}$ and assume that the order of σ is $p > 1$. Then $\Psi = \cup_{i=1}^{q} \langle \sigma \rangle \psi_i$ where $q \geq 1$ and $\{\psi_i \mid i = 1, 2, \ldots, q\}$ a complete set of coset representatives of $\langle \sigma \rangle$ in Ψ. By [7, Lemma 10.1.1],

$$\sum_{j=0}^{p-1} \sigma^j(\psi_i(s)) = \psi_i(s) + \sigma(\psi_i(s)) + \cdots + \sigma^{p-1}(\psi_i(s)) = 0$$

for $i = 1, 2, \ldots, q$. Recall that $\overline{b} = \overline{0}$, i.e. $b \in V$. Since V is contained in the center of N, we have

$$\begin{aligned} 0 = f\Big(\sum_{i=1}^{q} \big(\sum_{j=0}^{p-1} \sigma^j\big(\psi_i(s)\big)\big)\Big) &= \sum_{i=1}^{q} \Big(\sum_{j=0}^{p-1} f\big(\sigma^j\big(\psi_i(s)\big)\big)\Big) \\ &= \sum_{i=1}^{q} \Big(\sum_{j=0}^{p-1} \big(\theta(\sigma^j\psi_i)(a) + b\big)\Big) = \Big(\sum_{i=1}^{q} \big(\sum_{j=0}^{p-1} \theta(\sigma^j\psi_i)(a)\big)\Big) + kb. \end{aligned}$$

Suppose for now that θ is a homomorphism, i.e.

$$\theta(\psi_1\psi_2) = \theta(\psi_1)\theta(\psi_2) \quad \text{for all } \psi_1, \psi_2 \in \Psi. \tag{4.3}$$

Then $\theta(\sigma)$ and σ have the same order, and

$$\sum_{j=0}^{p-1} \theta(\sigma^j\psi_i)(a) = \sum_{j=0}^{p-1} \theta(\sigma)^j(\theta(\psi_i)(a)) = 0 \quad \text{for } i = 1, 2, \ldots, q.$$

In this case, we would have

$$\sum_{i=1}^{q}\sum_{j=0}^{p-1} \theta(\sigma^j\psi_i)(a) = 0,$$

and so $kb = 0$. Since N does not contain elements of order k, we could conclude that $b = 0$, which is certainly contradicting (4.1); the search would then be over.

Let us now prove (4.3). From $f(\psi(s)) = \theta(\psi)(a) + b$ we have

$$\widehat{f}(\widehat{\psi}(\overline{s})) = \widehat{\theta(\psi)}(\overline{a}) = \widehat{\theta(\psi)}(\widehat{f}(\overline{s})),$$

or equivalently,

$$\widehat{\psi}(\overline{s}) = (\widehat{f}^{-1}\widehat{\theta(\psi)}\widehat{f})(\overline{s}).$$

By induction, $\widehat{f}^{-1}\widehat{\Phi}\widehat{f} = \widehat{\Psi}$ which is a regular group of automorphisms of M/U. Thus, since $\overline{s} \neq \overline{0}$, we have

$$\widehat{\psi} = \widehat{f}^{-1}\widehat{\theta(\psi)}\widehat{f}, \quad \text{or} \quad \widehat{\theta(\psi)} = \widehat{f}\widehat{\psi}\widehat{f}^{-1}.$$

It follows that, for $\psi_1, \psi_2 \in \Phi$,

$$\widehat{\theta(\psi_1\psi_2)} = \widehat{f}(\widehat{\psi_1\psi_2})\widehat{f}^{-1} = (\widehat{f}\widehat{\psi}_1\widehat{f}^{-1})(\widehat{f}\widehat{\psi}_2\widehat{f}^{-1}) = \widehat{\theta(\psi_1)}\widehat{\theta(\psi_2)}.$$

Since $\widehat{\theta(\psi_1\psi_2)}, \widehat{\theta(\psi_1)}\widehat{\theta(\psi_2)} \in \widehat{\Phi}$ and the mapping $\widehat{\cdot} : \Phi \to \widehat{\Phi}$ given by $\varphi \mapsto \widehat{\varphi}$ is an isomorphism, we have $\theta(\psi_1\psi_2) = \theta(\psi_1)\theta(\psi_2)$ as required. The proof is now complete. $\square$

Now we prove the Main Theorem.

Proof of Main Theorem. Let $\overline{v} = |N/[N,N]|$.

We first consider the case $k > 6$. Notice that $(N/[N,N], \widehat{\Phi})$ is a Ferrero pair, and so $\frac{\overline{v}-1}{k}$ is an integer. Since $\frac{6}{k} < 1$, we have

$$2k^2 - 6k < \overline{v} - 1 \iff 2k - 6 + \frac{6}{k} < \frac{\overline{v}-1}{k} \iff 2k^2 - 6k + 6 < \overline{v} - 1.$$

Then the result follows from the Theorem 4.1.

Let $3 \leq k \leq 6$. Then Φ and Ψ are cyclic since k is a product of at most two primes (see [9, (I.5.2)]).

If k is even, then N and M are abelian by [7, Thm. 10.1.4]. Theorem 1 applies to show the result. Notice that the case $k = 2$ is trivial.

For $k = 5$, the only relevant numbers for $\overline{v}$ not covered by (N1) and Theorem 4.1 are $\overline{v} = 21$ and $\overline{v} = 26$. Both numbers are impossible as Φ acts on the Sylow-subgroups of $N/[N,N]$ by (N2).

In the case $k = 3$, Theorem 4.1 shows the claim. Notice that the bound gives $\overline{v} > 1$ which is trivially true. $\square$

5. The bound

Let (N, Φ) be an arbitrary finite Ferrero pair. As N is nilpotent, $(N/[N,N], \widehat{\Phi})$ is a Ferrero pair as well, where $\widehat{\Phi}$ is the fixed point free automorphism group consisting the automorphisms induced from those in Φ. Thus, $\Phi \cong \widehat{\Phi}$. If N is not abelian, then $N/[N,N]$ is abelian with $|N/[N,N]| < |N|$. For the quality of the bound, it suffices to consider $N/[N,N]$ instead of N. Thus, we may assume that N is abelian. In this case, there exists a characteristic elementary abelian subgroup N' in N, and again (N', Φ) is a Ferrero pair with $|N'| \le |N|$. Hence, we can safely assume that N is an elementary abelian p-group for some prime p. Further, as M and N are isomorphic groups in all cases we are interested in, without loss of generality, we may assume $M = N$.

Let the order of N be $q = p^\nu$. We define

$$K_q := \min\left\{k \in \mathbb{N} \mid k \text{ divides } (q-1) \text{ and } 2k^2 - 6k + 1 \ge q\right\}.$$

Thus, K_q is the smallest number k exceeding the bound such that there exists a group Φ of order k acting fixed point freely on N. For example, take $F = \mathrm{GF}(q)$, the Galois field of order q. Then N is isomorphic to the additive group of F while the cyclic subgroup Φ of $F \setminus \{0\}$ of order k acts on N fixed point freely.

Moreover, let $\bar{K}_q$ be the smallest k dividing $(q-1)$ and exceeding the bound such that there actually exist non-equivalent fixed point free subgroups Φ and Ψ in $\operatorname{Aut} N$ with isomorphic designs. By definition, we have $K_q \le \bar{K}_q$.

We start with a simple observation.

Lemma 5.1. *For every prime power q we have $K_q > \frac{\sqrt{2}}{2}\big(\sqrt{q}+1\big)$.*

Proof. For $k \in \mathbb{N}$ with $2k^2 - 6k + 1 \ge q$ we have

$$k \ge \frac{3}{2} + \frac{\sqrt{2}}{2}\sqrt{q + \frac{7}{2}} = \frac{\sqrt{2}}{2}\left(\frac{3\sqrt{2}}{4} + \sqrt{q}\cdot\sqrt{1+\frac{7}{2q}}\right) > \frac{\sqrt{2}}{2}\big(\sqrt{q}+1\big).$$

Hence the result. □

Proposition 5.2. *Let α be a rational number with $\alpha > \frac{\sqrt{2}}{2}$. Then there exist infinitely many primes p such that $K_{p^2} \le \alpha(p+1)$. Consequently, K_{p^2} can be arbitrarily close to $\frac{\sqrt{2}}{2}(p+1)$.*

Proof. For a prime p, set $k_p = \alpha(p+1)$. We'll show that there exist infinitely many primes p such that k_p is an integer satisfying the conditions in the definition of K_{p^2}.

Write $\alpha = \frac{a}{b}$ such that $a, b \in \mathbb{N}$ are relatively prime. Thus there exist $u, v \in \mathbb{Z}$ with $ua + vb = 1$. Then every $r \in \mathbb{Z}$ satisfying $r \equiv -ua + vb \pmod{ab}$ has the properties

$$r \equiv -1 \pmod{b}, \qquad r \equiv 1 \pmod{a}, \qquad \gcd(r, ab) = 1. \tag{5.1}$$

By Dirichlet's theorem on primes in arithmetic progressions [5, (VIII.4.1), p. 297] there exist infinitely many primes p with this property. We thus have, for these p's, $k_p \in \mathbb{N}$ and $k_p \,\big|\, (p^2-1)$. Moreover,

$$2\Big(k_p\big(k_p-3\big)\Big)+1 = 2k_p^2-6k_p+1 \geq p^2 \iff 2\alpha^2\left(1-\frac{3}{\alpha(p+1)}\right) \geq \frac{p-1}{p+1}.$$

The inequality on the right hand side holds when p is large enough. Thus there are infinitely many primes p with $K_{p^2} \leq \alpha(p+1)$. For such a p, we have

$$\frac{\sqrt{2}}{2}(p+1) < K_{p^2} \leq k_p = \alpha(p+1)$$

by Lemma 5.1. Since α can be arbitrarily close to $\frac{\sqrt{2}}{2}$, the proof is complete. $\square$

Table 5.1 on the right shows some numeric values of the smallest prime p_α with $K_{p_\alpha^2} \leq \alpha(p_\alpha+1)$ for the first convergents α of the continued fraction expansion of $\frac{\sqrt{2}}{2}$. Note that convergents of odd order are smaller than $\frac{\sqrt{2}}{2}$ and are therefore omitted.

Table 5.1

α	p
5/7	181
29/41	8,527
169/239	1,178,269
985/1393	9,840,151
5741/8119	334,275,467
33461/47321	36,690,053,423

For each α in the table, there are infinitely many primes satisfying (5.1). Let p_s the smallest one. We notice that $p_\alpha = p_s$ in all cases in the table but the first case $\alpha = 5/7$, where $p_s = 41$. It seems to be rare that p_s and p_α are distinct. For the first 19 examples we have checked, there is only one other instance.

Finally, we remark that if p satisfies the conditions in (5.1), so does p^ν for all odd ν.

6. Examples

In this section, we give some examples of nonequivalent Ferrero pairs with isomorphic design groups. The examples are based on certain Galois fields and the nearfields coupled to them. Readers who are interested in the theory on nearfields is referred to the book by Wähling [9]. We remark that Peter Mayer[1] has constructed some examples as well. These nonequivalent Ferrero pairs are not from nearfields, and give rise to isomorphic design groups.

We will need the following lemma. Here the notation $p^r \,\|\, n$ means that $p^r \,\big|\, n$ but $p^{r+1} \nmid n$.

[1]Private communication.

Lemma 6.1 ([9, (B.1.c),(B.2)]). *Let q and n be positive integers with $q \geq 2$.*

(1) *If $d \mid n$ and $\frac{q^n-1}{n} \leq q^d - 1$, then $d = n$.*

(2) *Let p be a prim divisor of $q-1$ such that $p^r \parallel (q-1)$ and $p^s \parallel n$.*
   (a) *If $p^r \neq 2$ or $s = 0$ then $p^{r+s} \parallel (q^n - 1)$.*
   (b) *If $p^r = 2$ and $s > 0$ then $2^{s+2} \mid (q^n - 1)$.*

Let q be a prime power and let $K = GF(q)$, the Galois field of q elements, and let $n > 1$ be an integer such that for all primes p and for $p = 4$, $p \mid n$ implies $p \mid (q-1)$. This pair (q, n) is called a *Dickson pair.* Then (and only then) the field $F = GF(q^n)$ allows a coupling $\kappa : F \to \mathrm{Aut}_K F; a \mapsto \kappa_a$ such that a nearfield multiplication on F can be defined. This nearfield, denoted as $F^\kappa = (F, +, \circ)$, has K as the kernel, i.e. $K = \{a \in F^\kappa \mid (x+y)\circ a = x\circ a + y \circ a\}$. Recall that the multiplication "$\circ$" in F^κ is given by

$$a \circ b = a \cdot \kappa_a(b) \quad \text{for all } a, b \in F^\kappa,$$

where $\cdot$ is the multiplication of F. Notice that $U_\kappa = \{a \in F^*;\ \kappa_a = \mathrm{id}\}$, the kernel of the coupling κ, has size $\frac{q^n-1}{n}$. See [9, IV §1] for details and proofs.

Assume now that we have a positive integer m such that

$$m \mid (q-1) \quad \text{and} \quad \gcd(m, n) = 1,$$

and put $k = \frac{q^n-1}{m}$. Let Φ be the cyclic subgroup of F^* of order k.

We shall derive some number theoretical statements before going into the examples. As $\gcd(n, m) = 1$, it's easy to see that

$$\gcd\left(\frac{q^n-1}{n}, \frac{q^n-1}{m}\right) = \frac{q^n-1}{nm}, \text{ hence } |U_\kappa \cap \Phi| = \frac{q^n-1}{nm}. \tag{6.1}$$

Furthermore, we'll show

$$|K^* \cap \Phi| = \gcd\left(q-1, \frac{q^n-1}{m}\right) = \frac{q-1}{m}\ . \tag{6.2}$$

The first equality is obvious since F^* is a cyclic group. Clearly $\frac{q-1}{m} \mid \gcd(q-1, k)$. Now let p be a prime divisor of $q-1$ and $p^r \parallel (q-1)$. If $p \nmid m$ we have $p^r \mid \frac{q-1}{m}$. If $p \mid m$ then $p \nmid n$. Hence using Lemma 6.1.(2) we see that $\gcd(q-1, k) \mid \frac{q-1}{m}$. Thus (6.2) holds.

Now, since Φ is characteristic, $\Phi^\kappa = (\Phi, \circ)$ is a subgroup of $(F^\kappa)^*$. We claim that

(1) Φ^κ is nonabelian.

This would mean that the groups Φ and Φ^κ are not isomorphic; therefore the Ferrero pairs (F, Φ) and (F^κ, Φ^κ) are not equivalent.

Using (6.1), we have

$$|\Phi/(\Phi \cap U_\kappa)| = n = |\mathrm{Aut}_K F|.$$

This says that the restriction of κ to Φ is surjective. Choose $a \in \Phi$ such that $\kappa_a(x) = x^q$ for all $x \in F$. Next, by Lemma 6.1.(1), we have $\frac{q^n-1}{n} \nmid (q-1)$. Together with (6.1) and (6.2), this implies $U_\kappa \cap \Phi \not\subseteq K^* \cap \Phi$. Therefore, there exists $b \in \Phi$ such that $b \cdot a^{-1} \in U_\kappa \setminus K$. The last relation means $\kappa_a = \kappa_b$. Assume that $a \circ b = b \circ a$ in F^κ. Then

$$a \cdot b^q = a \cdot \kappa_a(b) = a \circ b = b \circ a = a \cdot \kappa_a(b) = b \cdot a^q$$

and so $a^{q-1} = b^{q-1}$. But then $a \cdot b^{-1} \in K$, a contradiction. Thus $a \circ b \neq b \circ a$ and Φ^κ cannot be abelian.

Next, we show that

(2) $(F, \mathbf{B}_\Phi) = (F^\kappa, \mathbf{B}_{\Phi^\kappa})$.

This would mean that (F, Φ) and (F^κ, Φ^κ) are nonequivalent Ferrero pairs yet the design groups are isomorphic (actually, the same!).

Let R be a set of representatives of $K^* \cap \Phi$ inside K^*. For $a, b \in R, a \neq b$, we have $a^{-1} \cdot b \notin \Phi$, hence $\Phi a \neq \Phi b$. From (6.2) we have $|K^* \cap \Phi| = \frac{q-1}{m}$, therefore $|R| = |K^*/(K^* \cap \Phi)| = |F^*/\Phi|$. Consequently, R is also a set of coset representatives of Φ in F^*. Moreover, for all $\phi \in \Phi$ and all $r \in R$ we have $\phi \circ r = \phi\kappa_\phi(r) = \phi r$; thus $\Phi^\kappa \circ r = \Phi \cdot r$. Consequently, $(F, \mathbf{B}_\Phi) = (F^\kappa, \mathbf{B}_{\Phi^\kappa})$ as claimed.

Summarizing, we have shown

Theorem 2. *Let (q, n) be a Dickson pair and let m be a positive integer such that m divides $(q-1)$ and $\gcd(m, n) = 1$. Let $K = \mathrm{GF}(q)$, $F = \mathrm{GF}(q^n)$, and $\kappa : F \to \mathrm{Aut}_K(F)$ be a coupling of F such that the kernel of the nearfield F^κ is K. Let $k = \frac{q^n-1}{m}$ and let Φ be the subgroup of F^* with order k. Then Φ^κ is a subgroup of $(F^\kappa)^*$, and the Ferrero pairs (F, Φ) and (F^κ, Φ^κ) are not equivalent yet the design groups $(F, \mathbf{B}_\Phi, +)$ and $(F^\kappa, \mathbf{B}_{\Phi^\kappa}, +)$ are identical.*

Thus, for a Dickson pair (q, n), if there exists a prime divisor of $q-1$ not dividing n, then Theorem 2 gives us the desired examples. In this case we can choose a maximal m with the stated properties, and the resulting k would be minimal in the construction. More specific, our construction gives

Corollary 6.2. *Let (q,n) be a Dickson pair such that $w = \prod_{\substack{p|n \\ p^\nu \| (q-1)}} p^\nu > 1$, and put $m = (q-1)/w$. Then $\bar{K}_{q^n} \leq \frac{q^n-1}{m}$.*

Since for q an odd prime power $(q,2)$ is a Dickson pair, we obtain

Corollary 6.3. *Let q be a prime power. If $q \equiv -1 \pmod 4$, then $\bar{K}_{q^2} \leq 2(q+1)$.*

For the minimal k in Corollary 6.2, we find $k > \frac{q^n-1}{q}$ and so $k \geq q^{n-1}$. As the bound is roughly of order $q^{\frac{n}{2}}$, it is clear that only the case $n = 2$ can yield examples which are close to the bound. Therefore the statement in Corollary 6.3 is as close to the bound as we can get using our construction.

Remark 6.4. It's easy to see that $K_q \leq q+1$ for all prime powers $q > 2$. However, the above construction does not give examples, since Φ^κ is cyclic for $|\Phi| = q+1$. Moreover, it is conjectured that nonabelian Φ's of size $q+1$ are never circular, while abelian Φ's are, so the corresponding designs cannot be isomorphic.

Finally, we show that the Corollary to the Main Theorem also requires a bound.

Theorem 6.5. *Let K, F, κ, and Φ be as given in Theorem 2, and assume that $n \nmid (q-1)$. Then Φ^κ is not normal in the normalizer of Φ in $Aut(F,+)$. Therefore, $Aut(F^\kappa, \mathbf{B}_{\Phi^\kappa}, +)$ strictly contains the normalizer of Φ^κ.*

Proof. First notice that Φ generates F as a field since $\frac{q^n-1}{m} > q^{n-1}$. As $(F^\kappa, \mathbf{B}_{\Phi^\kappa}) = (F, \mathbf{B}_\Phi)$, from [8, (4.1)] we have

$$\mathrm{Aut}\,(F^\kappa, \mathbf{B}_{\Phi^\kappa}, +) = \mathrm{Aut}\,(F, \mathbf{B}_\Phi, +) = \Gamma L_F(F) = F^* \rtimes \mathrm{Aut}\,F$$

which is the normalizer of Φ inside $\mathrm{Aut}\,(F,+)$.

Notice that the map

$$(F^\kappa)^* \to F^* \rtimes \mathrm{Aut}\,F\,;\ a \mapsto (a, \kappa_a)$$

is a natural embedding.

Let $a \in \Phi$ be such that $\kappa_a(x) = x^q$. Then for $b \in F$ we have

$$(b,\mathrm{id})^{-1}(a,\kappa_a)(b,\mathrm{id}) = (b^{-1}a\kappa_a(b), \kappa_a) = (b^{q-1}a, \kappa_a).$$

This is in F^κ if and only if $\kappa_{b^{q-1}a} = \kappa_a$, and equivalently, if and only if $b^{q-1} \in U_\kappa$ (see [9, IV.1.1]). However, as $n \nmid (q-1)$ we have $b^{q-1} \notin U_\kappa$ for all generators b of F^*. $\square$

References

[1] K. I. Beidar, W.-F. Ke, C.-H. Liu, and W.-R. Wu. *Automorphism groups of certain simple 2-$(q, 3, \lambda)$ designs constructed from finite fields.* Finite Fields Appl. **9** (2003), 400–412.

[2] T. Beth, D. Jungnickel and H. Lenz. Design Theory. Cambridge Univ. Press, Cambridge, 1983.

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

[4] J. R. Clay. Nearrings: Geneses and Applications. Oxford Univ. Press, Oxford, 1992.

[5] A. Fröhlich and M. J. Taylor. Algebraic Number Theory. Cambridge Univ. Press, Cambridge, 1991.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2005, (`http://www.gap-system.org`).

[7] D. Gorenstein. Finite groups. Second edition. Chelsea Publishing Co., New York, 1980.

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

[9] H. Wähling, *Theorie der Fastkörper.* Thales Monographs 1. Thales-Verlag, Essen, 1987.

Wen-Fong Ke, Department of Mathematics, National Cheng Kung University, Tainan 701, Taiwan

E-mail address: `wfke@mail.ncku.edu.tw`

Hubert Kiechle, Mathematisches Seminar, Universität Hamburg, Bundesstr. 55, D-20146 Hamburg, Germany

E-mail address: `kiechle@math.uni-hamburg.de`