CONSTRUCTION OF FERRERO PAIRS OF ALL POSSIBLE ORDERS

TIM BOYKETT*

Abstract.
The structure of Ferrero pairs in terms of the sizes of the groups involved is investigated and an explicit condition is obtained. For every pair of numbers satisfying this criterion, a Ferrero pair is constructed explicitly. Thus the determination of interesting Ferrero pairs cannot be determined from their direct numerical properties.

Key words. Ferrero pairs, construction, nearrings

AMS subject classifications. 16Y30, 20B25, 20D45

1. Introduction. The use of planar nearrings to construct BIBDs dates back to Ferrero's initial paper [2]. One can say that the complete structure of the planar nearring and the BIBD is held within the structure of the Ferrero pair.

We look at the class of Ferrero pairs that can be constructed, characterising them by a simple parameter pair, and we see that all possible parameter pairs can be constructed explicitly using the field generated Ferrero pairs as building blocks.

A *Ferrero pair* (N, Φ) is an additively written (but not necessarily abelian) group N and a group Φ of fixed point free (also known as regular or semi–regular) automorphisms of N. We consider only finite N. The *parameters* of a Ferrero pair are $n = |N|$ and $t = |\Phi|$. Ferrero pairs are closely related to planar nearrings [1].

Ferrero pairs can be constructed from finite fields in a rather elementary manner. This construction dates back to Ferrero's original construction. Given a finite field K and some multiplicative subgroup $\Phi \leq K^*$, we see that Φ acts upon the additive group K as a group of fixed point free automorphisms. Thus we obtain a Ferrero pair (K, Φ). Such Ferrero pairs are known as *field generated Ferrero pairs*.

The main result of this paper is the following.

Theorem 1.1. *Let n, t be positive integers, $n = \Pi_i p_i^{e_i}$ the prime factorisation of n, then there exists a Ferrero pair (N, Φ) with $n = |N|$ and $t = |\Phi|$ iff t divides $p_i^{e_i} - 1$ for all i.*

We will go about obtaining this result by looking at what numbers n, t can exist, then explicitly constructing examples where these numbers are realised.

2. Obtaining Ferrero pairs. It would be of interest to be able to find suitable Φ for a given additive group N such that (N, Φ) is a Ferrero pair. In particular, we would like to know, for a given $n = |N|$, which values of $t = |\Phi|$ are theoretically possible and which can be explicitly constructed.

In this section we will see that a Ferrero pair can be decomposed into a collection of Ferrero pairs with n a prime power. We obtain some simple restrictions upon the values if t that are feasible. Then we will see an explicit construction for all pairs (n, t) that satisfy these constraints.

Proposition 1 (1.3 in [3]). *If (N, Φ) is a Ferrero pair with $N = N_1 \oplus N_2$ and Φ fixing the subgroups N_1 and N_2 as sets, then there are $\Phi_1 \cong \Phi_2 \cong \Phi$ such that (N_1, Φ_1) and (N_2, Φ_2) are Ferrero pairs.*

* Time's Up, Industriezeile 33b, A-4020 Linz, Austria, also Mathematik, Uni Linz, A-4040 Linz, Austria. `tim@timesup.org`

Proof: Let $\Phi_i := \Phi|_{N_i}$. For $\phi \in \Phi$, write $\phi_i := \phi|_{N_i}$. Suppose Φ_1 was not isomorphic to Φ. Then since Φ_1 is a homomorphic image of Φ, there is some non–identity $\phi \in \Phi$ such that ϕ_1 is the identity on N_1. Then $\phi(n_1, 0) = (\phi_1 n_1, \phi_2 0) = (n_1, 0)$ so $(n_1, 0)$ is a fixed point of ϕ. But ϕ is fixed point free, so $\Phi_i \cong \Phi$ for all i.

Suppose there is some $\phi_1 \in \Phi_1$ with a fixed point $n_1 \in N_1$, i.e. $\phi_1 n_1 = n_1$. Take ϕ the isomorph to ϕ_1 in Φ. Then $\phi(n_1, 0) = (\phi_1 n_1, \phi_2 0) = (n_1, 0)$ so $(n_1, 0)$ is a fixed point of ϕ. But (N, Φ) is a Ferrero pair, so this is not possible, thus there are no fixed points for any $\phi_1 \in \Phi_1$, and similarly for Φ_2, and we see that (N_i, Φ_i) is a Ferrero pair for each i. □

The restriction to two summands in the above is of course unnecessary, the result can easily be extended to many summands. The distinction of the Φ_i is also unnecessary since they are all isomorphic.

Corollary 2.1. *If (N, Φ) is a Ferrero pair and $N = \bigoplus_i N_i$ with each N_i Φ–invariant, then (N_i, Φ) is a Ferrero pair for each summand N_i.*

This becomes most interesting when we consider a Ferrero pair (N, Φ) and notice that because N is nilpotent by Thompson's theorem (see e.g.[4, p.306]), then it can be expressed as a direct product of its Sylow p–subgroups. Since an automorphism cannot take an element outside of its p–group, each Sylow subgroup is closed with respect to Φ. Thus Corollary 2.1 applies, and we can split the Ferrero pair up into a collection of non-interacting pairs.

Corollary 2.2. *A Ferrero pair is a direct sum of prime power Ferrero pairs with isomorphic automorphism groups.*

What is even more interesting is that the reverse construction also works.

Proposition 2 (5.42 in [1]). *Given a family (N_i, Φ_i) of Ferrero pairs with $\Phi_i \cong \Phi_j$ for all $i, j = 1, \ldots, k$, then (N, Φ) is also a Ferrero pair, where $N := \bigoplus_i N_i$ and $\Phi \cong \Phi_i$.*

The following two results form the proof of Theorem 1.1.

Corollary 2.3. *Given a Ferrero pair (N, Φ), with $n = |N| = \prod_i p_i^{e_i}$ as the prime factorisation, then $t = |\Phi|$ divides $p_i^{e_i} - 1$ for each i.*

Proof: Take one of the direct summands N_i of N as a sum of its Sylow subgroups and note that every orbit of Φ upon N_i except the 0–orbit has order t. No orbit can be larger, and if some orbit is smaller, then some $\phi \in \Phi$ has a fixed point in the orbit. Thus t divides $|N_i| - 1 = p_i^{e_i} - 1$ for each i and we are done. □

Proposition 3. *Given a number $n = \prod_i p_i^{e_i}$ and some number t such that t divides $p_i^{e_i} - 1$ for all i, there is a Ferrero pair (N, Φ) with $|N| = n$ and $|\Phi| = t$.*

Proof: Let $K_i := GF(p_i^{e_i})$ and $N_i := (K_i, +)$. Let ω_i be a generator of the multiplicative group K_i^*. Since t divides $p_i^{e_i} - 1$, let m_i be the number such that $m_i t = p_i^{e_i} - 1$. Then let $\Phi_i := < \omega_i^{m_i} >$, a cyclic subgroup of the multiplicative group K_i^* of order t. Then (N_i, Φ_i) is a field generated Ferrero pair.

Take $N := \bigoplus_i N_i$, Φ the cyclic group of order t and by Prop 2, (N, Φ) is a Ferrero pair with parameters (n, t). □

Thus we obtain Theorem 1.

3. Conclusion. In this note we have seen that there is an explicit construction method for Ferrero pairs of all possible orders. Thus the determination of the "interesting" Ferrero pairs cannot be based upon their numerical properties.

It is unknown whether the construction presented here of glueing Ferrero pairs together via their automorphism groups has a parallel in design theory.

4. Acknowledgements. The work that led to these results was funded by FWF Project P11486–TEC. I am grateful for resources offered by the Mathematics Department at the University of Western Australia, and funding from the Johannes–Kepler University Hochschulefonds financing as well as support from the Scientific Research funding of the government of Upper Austria.

REFERENCES

[1] James R. Clay. *Nearrings: Geneses and applications.* Oxford University Press, 1992.
[2] Giovanni Ferrero. Stems planari e BIB–desegni. *Riv. Mat. Univ. Parma*, pages 79–96, 1970.
[3] W-F Ke and H Keichle. Automorphisms of certain design groups. *J. Algebra*, 167:488–500, 1994.
[4] Derek J.S. Robinson. *A course in the theory of groups.* Springer, 1996.