On the Classification of Finite Nearfields

Christoph Hering

Mathematisches Institut, Universität Tübingen, Auf der Morgenstelle 10, 72076
Tübingen, Germany

Communicated by Gernot Stroth

Received April 18, 2000

TO HELMUT WIELANDT, TO COMMEMORATE HIS 90TH BIRTHDAY,
DECEMBER 19, 2000

The finite nearfields can be classified using R. Brauer’s result on finite linear
groups whose orders are divisible by large primes, together with some elementary
number theory. © 2000 Academic Press

A nearfield is an algebraic structure consisting of a set \( N \neq \emptyset \) together
with binary operations \( + \) and \( \cdot \) on \( N \) such that \((N, +)\) is a group with
identity element \( 0 \), \( x \cdot y \neq 0 \) for \( x, y \in N \setminus \{0\} \), \((N \setminus \{0\}, \cdot)\) is a group, and
furthermore \( x \cdot 0 = 0 \) and \( (x + y) \cdot z = x \cdot z + y \cdot z \) for all \( x, y, z \in N \). In
fact, a nearfield is essentially the same as a group with an automorphism
group acting sharply transitive on its non-trivial elements.

In 1935 Zassenhaus [12] classified the finite nearfields. The complicated
and long proof provides one of the first deep group theoretical classifica-
tions. It is remarkable that this early group theoretical result can also be
obtained with the help of the modular representation theory developed by
R. Brauer roughly at the same time.

Actually, Zassenhaus proved more than is necessary to characterise the
finite nearfields. He essentially characterised automorphism groups of finite
groups which are semiregular on the set of non-trivial elements. Our proof
is more general in another direction. We classify automorphism groups \( G \) of
a finite group \( V \) such that \( G \) is transitive on the set of non-trivial elements of
\( V \) and the order of \( G \) is prime to the order of \( V \).

More recent proofs of the result of Zassenhaus can be found in Passman
[9], Wolf [11], and Währing [10]. The notation in this paper is the same as
in [6].
Theorem 1. Let \( p \) be a prime, let \( F \) be a field of order \( p \), let \( V \) be a vector space of finite dimension \( n > 0 \) over \( F \), and let \( G \) be a subgroup of the general linear group \( GL(V, F) \) such that \( G \) is transitive on \( V \setminus \{0\} \) and \( p \nmid |G| \). Then \( G \) has an irreducible normal subgroup of prime order, unless \( p = 2 \) and \( n \in \{3, 4, 6, 8, 10, 12, 20\} \), or \( p = 3 \) and \( n \in \{4, 6\} \), or \( n = 2 \).

Proof. As \( G \) is transitive on the set of non-zero vectors of \( V \), \( \Phi_n^*(p) | p^n - 1 | |G| \). If \( \Phi_n^*(p) = 1 \), then \( n = 2 \) or \( n = 6 \) and \( p = 2 \) by Zsigmondy [13]. So we can assume that \( \Phi_n^*(p) \neq 1 \). Let \( r \) be a prime divisor of \( \Phi_n^*(p) \). We consider at first the case that \( G \) contains a group \( R \) of order \( r^2 \). As \( p \nmid |G| \), we can lift the matrix group \( G \) to characteristic 0 and then reduce it modulo \( r \) to obtain a homomorphism of \( G \) into \( GL(n, r^a) \) for some \( a \geq 1 \), whose kernel \( K \) is a r-group. Here \( r \equiv 1 \pmod{n} \) by [6, Theorem 3.5], so that \( r > n \) and hence the exponent of a Sylow r-subgroup of \( GL(n, r^a) \) is \( r \). Also, by [5, Korollar 1] every r-subgroup of \( G \) is cyclic. Therefore \( R \cap K \neq 1 \) and \( K \) contains a unique subgroup of order \( r \), which is an irreducible normal subgroup of \( G \).

Hence we can assume that \( G \) does not contain any subgroup of order \( r^2 \) and thus \( \Phi_n^*(p) \) is squarefree. We now apply Brauer’s theorem [1] to this situation. If \( r > 2n + 1 \) then \( G \) contains a normal Sylow r-subgroup, and we are finished.

Therefore we can assume that \( r \leq 2n + 1 \). As \( r \equiv 1 \pmod{n} \), there only remain the cases \( \Phi_n^*(p) = n + 1, 2n + 1, \) or \( (n + 1)(2n + 1) \). By [6, Theorem 3.9] this is only possible for finitely many values of \( p^n \). (At this point the (elementary) number theory comes in. [6, Theorem 3.9] is an extension of Zsigmondy’s theorem of 1892. By the way, the same result also is proved in a paper of Feit [4].)

The cases \( p^n = 2^{18}, 3^{18}, 5^6, \) or \( 17^6 \) can be tackled using the extension of Feit and Thompson of Brauer’s result. Let \( s \) be a prime divisor of \( \Phi_{n/2}^*(p) \) and let \( S \) be a Sylow \( s \)-subgroup of \( G \). In all four cases \( s > 2n + 1 \) so that \( S \leq G \) by Feit and Thompson [3]. As \( G \) is irreducible, the module \( (V, FS) \) has only one Wedderburn component. Therefore \( S \) is cyclic, the subalgebra of the endomorphism algebra of \( V \) generated by \( S \) is a field \( \overline{F} \) of order \( p^{n/2} \), and \( G \leq GL(V, \overline{F}) \). Here \( |GL(V, \overline{F}) : GL(V, \overline{F})| = 2 \) so that a Sylow r-subgroup \( R \) of \( G \) is contained in \( G \cap GL(V, \overline{F}) \). As \( r > 5 = 2 \cdot \dim(V, \overline{F}) + 1 \), \( R \leq G \cap GL(V, \overline{F}) \) by Brauer. Clearly \( R \) is characteristic in \( G \cap GL(V, \overline{F}) \) and hence normal in \( G \).

Theorem 2. Let \( F \) be a field of prime order \( p \), let \( V \) be a vector space of finite dimension \( n > 0 \) over \( F \), and let \( G \) be a subgroup of \( GL(V, F) \) acting sharply transitive on \( V \setminus \{0\} \). Then \( G \) contains an irreducible abelian normal subgroup, unless \( n = 2 \).
Proof. Assume \( n > 2 \). Then there remain only the finitely many cases listed in Theorem 1. Also, \( |G| = p^n - 1 \). Let \( r_1, \ldots, r_t \) be the prime divisors of \( |G| \) such that \( r_1 < r_2 < \cdots < r_t \). If \( p = 2 \), then by a famous result of Burnside [8, p. 499, 8.7], every Sylow subgroup of \( G \) is cyclic. Also, every Sylow \( r_1 \)-subgroup lies in the center of its normaliser and, again by Burnside [8, p. 420, 2.8], \( G \) has a normal \( r_1 \)-complement. Thus we obtain a series of characteristic subgroups

\[ G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_t = 1 \]

such that \( G_i \) is a normal \( r_i \)-complement in \( G_{i-1} \) for \( i = 1, \ldots, t \). If \( n = 6 \), then \( t = 2 \), \( r_2 = 7 \), and \( |\mathbb{Z}_G[G_1]| = 3 \cdot 7 \) or \( 3^2 \cdot 7 \), so that \( G \) contains a cyclic normal subgroup of order 21, which is irreducible. If \( n = 10 \), then \( t = 3 \) and \( |G_1| = 11 \cdot 31 \) so that \( G_2 \) is cyclic and \( G \) contains an irreducible normal subgroup of order 11. In the remaining cases \( r_i |\Phi^n(p) \) and \( G_{i-1} \) is an irreducible normal subgroup of prime order. We consider the case \( p = 3 \). Let \( r \) be a prime divisor of \( \Phi^n(p) \) and let \( R \) be a Sylow \( r \)-subgroup of \( G \). An involution in \( G \) does not fix any non-zero vector and hence equals \(-I\). So \( < -I > \times R \leq \mathbb{Z}_G[R] \) and the number of Sylow \( r \)-subgroups divides \( |G| / 2r \). By Sylow’s theorem we obtain \( R \leq G \).

If in Theorem 2 the group \( G \) contains an irreducible abelian normal subgroup \( A \), then the subalgebra of the endomorphism algebra of \( V \) generated by \( A \) is a field \( \mathbb{F} \) of order \( p^n \) and \( G \) is contained in \( \text{GL}(V, \mathbb{F}) \), the group of non-singular semilinear transformations of the one-dimensional vector space \( (V, \mathbb{F}) \) (see [7]). It is now not difficult to prove that the nearfield corresponding to \( G \) is a regular nearfield. If, on the other hand, \( n = 2 \), then \( G \) is a group of \( 2 \times 2 \)-matrices, and one can use Dickson’s classification of all subgroups of \( PSL(2, p) \) (see [8, p. 213, 8.27]). Actually, Dickson [2] in 1905 already determined the seven finite nearfields of dimension 2 which are not regular nearfields. Remarkably, although the situation looks very complicated in dimension 2, there are no irregular nearfields in higher dimension.

REFERENCES

1. R. Brauer, On groups whose order contains a prime number to the first power, II, Amer. J. Math. 64 (1942), 421–440.
3. W. Feit and J. G. Thompson, Groups which have a faithful representation of degree less than \( (p - 1)/2 \), Pacific J. Math. 11 (1961), 1257–1262.


