# Finite Nearfields in MAGMA

Don Taylor

29 February 2012

TEXed: 4 December, 2012

The content of this note is a literate MAGMA script illustrating the facility for user-defined types in MAGMA. The code defines three new types for finite nearfields and an associated element type. There is an 'abstract' type NFD and two derived types: NFDDCK for regular (Dickson) nearfields and NFDZSS for irregular (Zassenhaus) nearfields; they inherit the attributes declared for the NFD type. Both NFDDCK and NFDZSS use the same element type: NFDELT.

Nearfields are important in group theory, geometry and a combination of these two fields. On the one hand, the finite sharply doubly transitive permutation groups are in one-to-one correspondence with the finite nearfields and on the other hand, nearfields coordinatise a class of translation planes [29, 38] and they are the starting point for the construction of the Hughes planes [15, 31]. Furthermore, every sharply transitive collineation group of projective space over finite field is a quotient of the group of units of a nearfield [22] (see also, [14, §1.4, n° 17].

The code to implement the nearfield types was supplied by John Cannon.

## 1 User types

The following description of user types has been lifted from the documentation supplied by Allan Steel. These types are intended to replace the 'hackobj' types which are internal to MAGMA and not accessible to the average user. The instructions for removing 'hackobj' types and replacing them with user types is contained in the full documentation in the file `user_types.doc`.

### 1.1 Summary

- User types can now be declared in a package file.
- A type declaration may also specify ISA relations and an element type.
- A type declaration may be placed anywhere (but typically should be placed before an attributes declaration).

### 1.2 Declaring types

Let MYTYPE be the new type in the following (and similarly MYTYPE2, MYTYPE3, ...). The simplest form of a type declaration is:

```
declare type MyType;
```

If MyType is to inherit from types MyType2, MyType3, ..., then add them after a colon:

```
declare type MyType: MyType2, MyType3;
```

If MyTypeElt is the element type for MyType (i.e., if objects of type MyTypeElt have type MyType for their parents, so that a set or sequence whose universe has type MyType will contain elements of type MyTypeElt), then MyTypeElt should be placed in brackets after MyType as follows:

```
declare type MyType [MyTypeElt];

declare type MyType [MyTypeElt]: MyType2, MyType3; // ISA relations
```

If MyTypeElt is supplied, then a Parent intrinsic must be present for MyTypeElt (which must return objects of type MyType).

The type declaration can be placed *anywhere* in a package file and such a file can appear anywhere in a `spec` file. That is, the type may be referenced (particularly in signatures) in files that are attached before the file containing the type declaration. The only restriction is that the file declaring the type must be attached before any code is *run* which uses the type.

### 1.3 Standard intrinsics to be defined for user types

The following standard intrinsics should be defined for any user type MyType.

```
intrinsic Print(x::MyType)
```

or

```
intrinsic Print(x::MyType, level::MonStgElt)
```

or

```
intrinsic PrintNamed(x::MyType, level::MonStgElt, name::MonStgElt)
```

(Procedure) Print *x* of type MyType. A new line should *not* be printed at the end of the last (or only) line (thus one should use **printf**, etc.). If the second form of procedure is used, then *x* should be printed at the given level (the *level* argument is a string; test for equality with 'Maximal', etc.)

In the PrintNamed version, the string name of the object is given in the third argument. So the object *x* should be printed at the given level, using the name if desired, as in:

```
> Sym(2);
Symmetric group acting on a set of cardinality 2
> S:=Sym(2); S;
Symmetric group S acting on a set of cardinality 2
```

```
intrinsic IsCoercible(X::MyType, y::.) -> BoolElt, .
```

(Function) Attempt to coerce *y* into MyType *X*.
If successful: **return** true, *the_result* (which must be in *X*)
else: **return** false, `error-message-string`
If no coercion is allowable, make the body of the function be:
**return** false, `"Illegal coercion"`;

```
intrinsic 'in'(y::., X::MyType) -> BoolElt
```

(Function) Return whether the arbitrary object *y* is in MyType *X*. Simple true/false is the single return value). *Note* the order of the arguments!

```
intrinsic Parent(x::MyTypeElt) -> MyType
```

(Function) Return the parent of *x*. This is assuming that MyType was declared to have MyTypeElt as element type.

*Note*: If *T* is a type which is not an element type for any other type, then a parent function for objects of type *T* should *not* be defined; it will be automatically present, returning PowerStructure(*T*).

## 1.4 Optional intrinsics for user types

```
intrinsic SubConstr(X::MyType, RHS::<typeRHS> ) -> MyType, Map
intrinsic SubConstr(X::MyType, R1::<typeR1>, R2::<typeR2> )
   -> MyType, Map
```

(Function) Called when ***sub***$<X \mid \text{RHS}>$ or ***sub***$<X \mid R_1, R_2>$ is called. Specify $<$*typeRHS*$>$ to restrict types RHS or use . and check types within the function. The function *must not use* **require**/**error**; use:

```
return "error message", _;  // note the second return value
```

when there is an error or if RHS is wrong. The function should also return the subobject *S* and inclusion map: $S \to X$. The type of *S* and MyType must have an ISA relation.

```
intrinsic HomConstr(D::MyType, C::<typeC>, RHS::<typeRHS>:
         Check := false) -> Map
intrinsic HomConstr(D::MyType, C::<typeC>, R1::<typeR1>,
         R2::<typeR2>: Check := false) -> Map
```

(Function) These intrinsics are called when ***hom***$< D \to C \mid$ RHS: Check$>$ is called or when ***hom***$< D \to C \mid R_1, R_2$: Check$>$ is called. Specify $<$*typeC*$>$ or $<$*typeRHS*$>$ to restrict types of *C* and RHS or use . and check types within the function. Default value for Check is false and can't be changed on the Magma level. If Check is true, the function should check if RHS actually defines a homomorphism; if Check is false, the check isn't necessary. *Must not use* **require**/**error** (as above).

Intrinsics to create objects of type MyType can use the following expression

```
New(MyType);
```

to create an empty object of type MyType. Typically one would then set relevant attributes.

## 2 Nearfield properties

In 1905, in the course of proving the independence of the field postulates, L. E. Dickson [18, p. 203] introduced the first example of a nearfield. His example is a set of 9 elements with operations of addition and multiplication which satisfy all the axioms of a field except for the commutative law of multiplication and the right distributive law. Later that year Dickson [20] published a more extensive collection of examples: an infinite series obtained by twisting the multiplication of a Galois field and seven "irregular" examples.

The terminology 'nearfield' seems to have introduced by Zassenhaus in his 1935 paper [67] where he showed that the only finite nearfields (endliche Fastkörper) are those due to Dickson.

The irregular nearfields are often referred to as Zassenhaus nearfields and the nearfields in the infinite series are called Dickson nearfields.

In the papers of Dickson and Zassenhaus the nearfields are left-distributive but for the purposes of the MAGMA implementation we consider only right-distributive nearfields.

**Definition 2.1.** A (right-distributive) *nearfield* is a set $N$ containing elements 0 and 1 and with binary operations $+$ and $\circ$ such that

**NF1:** $(N, +)$ is an abelian group and 0 is its identity element. Let $N^\times$ denote the set of non-zero elements of $N$.

**NF2:** $(N^\times, \circ)$ is a group and 1 is its identity element.

**NF3:** $a \circ 0 = 0 \circ a = 0$ for all $a \in N$.

**NF4:** $(a + b) \circ c = a \circ c + b \circ c$ for all $a, b, c \in N$.

**Definition 2.2.** A subset $S$ of a nearfield $N$ is a *sub-nearfield* if $(S, +)$ and $(S \setminus \{0\}, \circ)$ are groups. The sub-nearfield *generated* by a subset $X$ is the intersection of all sub-nearfields containing $X$. The *prime field* $\mathcal{P}(N)$ of $N$ is the sub-nearfield generated by 1.

The inverse of $x \in N^\times$ is written $x^{[-1]}$. But where no confusion is possible we write multiplication of nearfield elements $x$ and $y$ as $xy$ rather than $x \circ y$ and we write the inverse of $x$ as $x^{-1}$. (In the MAGMA code we use $*$ as the symbol for multiplication.)

If $N$ is a finite nearfield, the prime field of $N$ is a Galois field $\mathrm{GF}(p)$ for some prime $p$, called the *characteristic* of $N$.

A nearfield of characteristic $p$ is a vector space over its prime field and therefore its cardinality is $p^n$ for some $n$. Every field is a nearfield.

**Definition 2.3.** If $N$ is a nearfield, the *centre* of $N$ is the set

$$\mathcal{Z}(N) = \{\, x \in N \mid xy = yx \text{ for all } y \in N \,\}$$

and the *kernel* of $N$ is the subfield

$$\mathcal{K}(N) = \{\, x \in N \mid x(y + z) = xy + xz \text{ for all } y, z \in N \,\}.$$

It is clear that $\mathcal{Z}(N) \subseteq \mathcal{K}(N)$ but equality need not hold because, in general, $\mathcal{Z}(N)$ need not be closed under addition. Furthermore, the prime field $\mathcal{P}(N)$ need not be contained in $\mathcal{Z}(N)$. However, for the Dickson nearfields defined below $\mathcal{Z}(N) = \mathcal{K}(N)$.

**Lemma 2.4.** *If $N$ is a nearfield, then $\mathcal{Z}(N) = \bigcap\{\mathcal{K}(N)^x \mid x \in N,\ x \neq 0\}$.*

*Proof.* (See [14]) If $L = \bigcap\{\mathcal{K}(N)^x \mid x \in N,\ x \neq 0\}$, it is clear that $\mathcal{Z}(N) \subseteq L$. To prove the converse, we may suppose that $\mathcal{K}(N) \neq N$ and choose $0 \neq t \in N \setminus \mathcal{K}(N)$. If $d \in L$, then there exist $d_1, d_2 \in L$ such that $td_1 = td$ and $(t+1)d = d_2(t+1)$. Thus

$$d_1 t + d = td + d = (t+1)d = d_2(t+1) = d_2 t + d_2,$$

whence $(d_1 - d_2)t = d_2 - d$. But $d_1 - d_2$ and $d_2 - d$ belong to $\mathcal{K}(N)$ and since $t \notin \mathcal{K}(N)$ it follows that $d_1 = d_2 = d$. That is, $td = dt$ and hence $L \subseteq \mathcal{Z}(N)$, as asserted. □

## 2.1 Sharply doubly transitive groups

**Definition 2.5.** A group $G$ acting on a set $\Omega$ is *sharply doubly transitive* if $G$ is doubly transitive on $\Omega$ and only the identity element fixes two points.

The finite sharply doubly transitive groups were determined by Zassenhaus [67] in 1935. Accounts of the classification can be found in many places, including most of the books listed in the references below. (Many recent references to Zassenhaus use 1936 as the publication date for this paper, perhaps because this issue of the journal did not appear until 1936.)

**Theorem 2.6.** *Suppose that $G$ is a finite sharply doubly transitive group on $\Omega$. Then*

*(1) The set $M$ consisting of the identity element and the elements of $G$ without fixed points is an elementary abelian normal subgroup of $G$ of order $p^n$ for some $n$ and some prime $p$.*

*(2) Addition and multiplication between elements of $\Omega$ can be defined so that $\Omega$ becomes a nearfield and so that the group $G$ is isomorphic to the group of all affine transformations $v \mapsto va + b$ of $\Omega$, where $a \in \Omega^\times$ and $b \in \Omega$.*

*Proof.* If $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$, then $G_\alpha \cap G_\beta = 1$ and therefore the conjugates of $G_\alpha$ contain $m(m-2)+1$ elements, where $m = |\Omega|$. Thus there are $m-1$ elements without fixed points and so $|M| = m$.

If $a \in M$ and $b \in C_G(a)$, then $b \in M$ otherwise $b$ would fix a unique point in $\alpha \in \Omega$ and then $a$ would also fix $\alpha$. Thus $C_G(a) \subseteq M$ and so $|G : C_G(a)| \geq m-1$. It follows that equality holds and so $M$ is a normal abelian subgroup of $G$ and its non-identity elements form a single conjugacy class in $G$. Consequently $M$ is an elementary abelian $p$-group for some prime $p$ and therefore $m = p^n$ for some $n$.

Choose two elements of $\Omega$ and label them 0 and 1. Let $H = G_0$. The group $M$ acts regularly on $\Omega$ and therefore for all $a \in \Omega$ there exists $\eta(a) \in M$ such that $a = 0^{\eta(a)}$. The map $\eta : \Omega \to M$ is a bijection such that for all $a \in \Omega$ and all $x \in H$ we have $\eta(a^x) = x^{-1}\eta(a)x$. Using $\eta$ we transfer the group structure of $M$ to $\Omega$ but write it additively. That is, for $a, b \in \Omega$, define $a + b \in \Omega$ so that $\eta(a+b) = \eta(a)\eta(b)$.

The group $H$ acts regularly on $\Omega^\times = \Omega \setminus \{0\}$ and therefore there is a bijection $\mu : \Omega^\times \to H$ such that $a = 1^{\mu(a)}$ for all $a \in \Omega^\times$. Now use $\mu$ to define multiplication on $\Omega^\times$; that is, for $a \in \Omega$ define $0a = a0 = 0$ and for $a, b \in \Omega^\times$, define $ab \in \Omega$ so that $\mu(ab) = \mu(a)\mu(b)$.

The right distributive law holds because $\eta(bc) = \eta(b^{\mu(c)}) = \mu(c)^{-1}\eta(b)\mu(c)$ and hence

$$ac + bc = (ac)^{\eta(bc)} = a^{\mu(c)\mu(c)^{-1}\eta(b)\mu(c)} = a^{\eta(b)\mu(c)} = (a+b)c.$$

Thus $\Omega$ is a nearfield. The group $G$ is the semidirect product $H \ltimes M$ of $M$ and $H$. Therefore, if $g \in G$ there exists unique elements $h \in H$ and $m \in M$ such that $g = hm$. Then $h = \mu(a)$ and $m = \eta(b)$, where $a \in \Omega^\times$ and $b \in \Omega$ and consequently for all $v \in \Omega$ we have

$$v^g = v^{\mu(a)\eta(b)} = va + b. \qquad \square$$

There is a converse to this theorem, namely if $N$ is a nearfield, the group of all transformations $v \mapsto va + b$ acts sharply doubly transitively on $N$.

Let $F$ be the prime field of $N$, regard $N$ as a vector space over $F$ and define $\mu : N^\times \to \mathrm{GL}(N)$ by $v^{\mu(a)} = va$. Then for all $a \in N^\times$, $a \neq 1$, the linear transformation $\mu(a)$ is fixed-point-free. Furthermore, $\mu$ defines an isomorphism between the multiplicative group $N^\times$ and its image in $\mathrm{GL}(N)$.

Suppose that $G = H \ltimes M$ is a sharply doubly transitive group of degree $p^n$, as above. The centre of $G$ is trivial and $M$ is a minimal normal subgroup. Thus if $\Omega'$ is a minimal permutation representation we may suppose that it is primitive. Then $M$ is transitive on $\Omega'$ and since $M$ is abelian, it acts regularly on $\Omega'$. Thus $p^n$ is the minimal degree of a faithful permutation representation of $G$.

# 3 The MAGMA code

## 3.1 Type declarations

There are two types of finite nearfield: the *regular* nearfields of Dickson and the *irregular* nearfields of Zassenhaus. In order to accommodate both types we declare a 'virtual type' NFD and then types NFDDCK and NFDZSS which inherit from NFD.

```
declare type NFD;
declare attributes NFD:
    gf,    // Underlying finite field
    prim,    // Primitive element of the underlying field
    p,    // Characteristic of the underlying finite field
    q,    // Order of the kernel of the nearfield
    matgrp,    // The matrix group of units of the nearfield
    sz,    // The size of the base field of matgrp
    ψ,    // Homomorphism from matgrp to the nearfield
    φ;    // Bijection between field and vector space
```

Objects of the derived types NFDDCK and NFDZSS will both have elements of type NFDELT and so we declare that type here.

```
declare type NFDELT;
declare attributes NFDELT:
    parent,    // Parent of element
    elt,    // Element (as an element of the corresponding finite field)
    log;    // Logarithm of the element, when a unit, otherwise -1
```

When declaring a user-defined type in MAGMA the element type is placed in brackets after the type name.

```
declare type NFDDCK [NFDELT]: NFD;
```

Derived types inherit the attributes of the parent type and so for NFDDCK and NFDZSS we need only declare the additional attributes specific to these types.

```
declare attributes NFDDCK:
    h, v,    // (p, h, v) is a Dickson triple
    twist,   // sequence twisted residues mod v
    ρ;   // sequence of Frobenius powers
declare type NFDZSS [NFDELT]: NFD;
declare attributes NFDZSS:
    ndx,    // The index of the irregular nearfield
    μ;   // Associative array mapping vectors to matrices
```

### 3.2 Dickson nearfields

In order to begin exploring the new types in MAGMA we need a way to create instances of nearfields and their elements. As already mentioned there is a large class of nearfields first described by L. E. Dickson [18, 20] in 1905 and in this section we provide a MAGMA intrinsic for their construction.

The nearfields resulting from this construction will be called *Dickson* (or *regular*) nearfields.

**Definition 3.1.** If $p$ is a prime and if the positive integers $h$ and $v$ satisfy

- *if $r$ is a prime or 4 and if $r$ divides $v$, then $r$ divides $p^h - 1$*

then $(p, h, v)$ is a *Dickson triple*.

If we write $q = p^h$, the condition above is equivalent to

- *All prime factors of $v$ divide $q - 1$ and $q \equiv 3 \mod 4$ implies $v \not\equiv 0 \mod 4$.*

We call $(q, v)$ a *Dickson pair*.

```
isDicksonPair := func< q, v |
   IsPrimePower(q) and forall{ r : r in PrimeBasis(v) | q mod r eq 1 } and
      ((q mod 4 eq 1) or (v mod 4 ne 0)) >;

intrinsic DicksonPairs(p :: RngIntElt, hlo :: RngIntElt, hhi :: RngIntElt,
                                vlo :: RngIntElt, vhi :: RngIntElt) → []
{List the Dickson pairs (q, v) for prime p, where hlo and hhi
 are the lower and upper bounds on h and vlo, vhi
 are the lower and upper bounds on v}
  require IsPrime(p): "p must be prime";
  pairs := [];
  for h := hlo to hhi do
     for v := vlo to vhi do
        if isDicksonPair(p^h, v) then
            Append(~pairs, [p^h, v]);
        end if;
     end for;
  end for;
  return pairs;
```

```
end intrinsic;

intrinsic DicksonPairs(p :: RngIntElt, h1 :: RngIntElt, v1 :: RngIntElt) -> []
{List the Dickson pairs (p^h, v) for prime p, where h1 and v1
 are upper bounds on h and v}
 return DicksonPairs(p, 1, h1, 1, v1);
end intrinsic;

intrinsic DicksonTriples(p :: RngIntElt, hb :: RngIntElt, vb :: RngIntElt) -> []
{List the Dickson triples (p,h,v) for prime p, where
 hb and vb are bounds on h and v}
  require IsPrime(p): "p must be prime";
  triples := [];
  for h := 1 to hb do
    for v := 1 to vb do
      if isDicksonPair(p^h, v) then
        Append(~triples, [p, h, v]);
      end if;
    end for;
  end for;
  return triples;
end intrinsic;
```

Given a Dickson pair $(q, v)$, the following function creates a raw object of nearfield type (NfdDck). More needs to be done before the object can be used as a nearfield. In particular, the operations of addition and multiplication need to be defined.

The isomorphism type of a Dickson nearfield depends on the choice of primitive element of the underlying Galois field. It has been shown by Lüneburg [39] that if $\phi$ is the Euler phi-function and $g$ is the order of $p$ modulo $v$, there are $\phi(v)/g$ isomorphism classes of Dickson nearfields with the same Dickson triple $(p, h, v)$.

```
good_exponent := function(q, v, e)
  m := (q^v - 1) div v;
  m_ := &*{ r : r in PrimeDivisors(m) | not IsDivisibleBy(e, r) };
  return e + m_*v;
end function;
```

For later use, when constructing sub-nearfields, it will be convenient to be able to specify the primitive element $\zeta$ directly.

```
nearField := function(q, v, K, ζ : LargeMatrices := false)
  _, p, h := IsPrimePower(q);
  sz := LargeMatrices select p else q;
  L := GF(sz);
  E, φ := VectorSpace(K, L);
  twist := [ 0 : j in [1..v]];
  ρ := twist;
  for i := 1 to v do
    s := ((q^i-1) div (q-1)) mod v;
    twist[s+1] := i;
```

```
    ρ[s+1] := q^i;
  end for;
```

The intrinsic New creates a new object of the given type.

```
  NF := New(NfdDck);
  NF`p := p;
  NF`h := h;
  NF`v := v;
  NF`q := q;
  NF`gf := K;
  NF`sz := sz;
  NF`φ := φ;
  NF`prim := ζ;
  NF`twist := twist;
  NF`ρ := ρ;
  return NF;
end function;
```

The default nearfield will use the 'standard' primitive element of the field. The other variants with the same Dickson pair can be obtained by providing an integer $s$ coprime to $v$. This must be converted to a suitable integer $e$ coprime to $q^v - 1$ such that $s \equiv e \mod v$ (see the proof of Lemma 4.2 for the details).

```
intrinsic DicksonNearfield(q :: RngIntElt, v :: RngIntElt : Variant := 1,
          LargeMatrices := false) -> NfdDck
{Create a Dickson nearfield from the Dickson pair (q,v)}
  require isDicksonPair(q,v):
        Sprintf("(%o, %o) is not a Dickson pair", q, v);
  e := (v eq 1) select 1 else Integers() ! Variant mod v;
  require IsCoprime(v,e): "Variant must be coprime to v";
  if e ne 1 then
    e := good_exponent(q,v,e);
  end if;
  K := GF(q^v);
  return nearField(q,v,K,PrimitiveElement(K)^e :
      LargeMatrices := LargeMatrices);
end intrinsic;

intrinsic NumberOfVariants(q :: RngIntElt, v :: RngIntElt) -> RngIntElt
{The number of non-isomorphic nearfields with
 Dickson pair (q,v)}
  require isDicksonPair(q, v):
        Sprintf("(%o, %o) is not a Dickson pair", q, v);
  if v eq 1 then return 1; end if;
  _, p, h := IsPrimePower(q);
  return EulerPhi(v) div Order(ResidueClassRing(v) ! p);
end intrinsic;

intrinsic NumberOfVariants(N :: NfdDck) -> RngIntElt
```

```
{The number of variants of the Dickson nearfield N}
  return EulerPhi(N`v) div Order(ResidueClassRing(N`v) ! N`p);
end intrinsic;

intrinsic VariantRepresentatives(q :: RngIntElt, v :: RngIntElt) -> SeqEnum
{Representatives for the variant parameter of nearfields with
  Dickson pair (q,v)}
  require isDicksonPair(q,v):
       Sprintf("(%o, %o) is not a Dickson pair", q, v );
  if v eq 1 then return [ 1 ]; end if;
  _, p, h := IsPrimePower(q);
  R := ResidueClassRing(v);
  U,f := UnitGroup(R);
  X := {@ f(u) : u in U @};
  π := R ! p;
  t := [ x*π : x in X ];
  S := Sym(X);
  P := sub<S|t>;
  reps := OrbitRepresentatives(P);
  return [r[2] : r in reps];
end intrinsic;
```

### 3.3 Irregular nearfields

It was shown by Zassenhaus [67] that in addition to the regular nearfields there are seven *irregular* nearfields. Zassenhaus gives constructions but does not prove their uniqueness.

The proofs in [67] are known to contain gaps. Perhaps the most reliable account of the existence and uniqueness of the irregular nearfields is the PhD thesis of Dancs-Groves [27].

The seven finite nearfields which are not Dickson nearfields will be called the *irregular* nearfields. To define them we first define seven matrix groups which act fixed-point-freely on the non-zero vectors of the underlying vector space.

Irregular nearfields can be distinguished from regular nearfields by the following property of their unit groups.

**Theorem 3.2** ([27, Lemma 4.16])**.** *The multiplicative group of a finite nearfield $N$ is metacyclic if and only if $N$ is regular.*

As a consequence, a Zassenhaus nearfield cannot occur as a subfield of a Dickson nearfield.

The matrices in the following function were obtained from Hall [29, p. 391]. Note that in [14] there is a misprint in the definition of the matrix $A$.

```
irrNF := function(ndx)
  A := Matrix(2,2,[0,1,-1,0]);
  case ndx:
     when 1:
        p := 5;
        B := Matrix(2,2,[1,-2,-1,-2]);
     when 2:
```

```
            p := 11;
            B := MATRIX(2,2,[1,5,-5,-2]);
            C := MATRIX(2,2,[4,0,0,4]);
        when 3:
            p := 7;
            B := MATRIX(2,2,[1,3,-1,-2]);
        when 4:
            p := 23;
            B := MATRIX(2,2,[1,-6,12,-2]);
            C := MATRIX(2,2,[2,0,0,2]);
        when 5:
            p := 11;
            B := MATRIX(2,2,[2,4,1,-3]);
        when 6:
            p := 29;
            B := MATRIX(2,2,[1,-7,-12,-2]);
            C := MATRIX(2,2,[16,0,0,16]);
        when 7:
            p := 59;
            B := MATRIX(2,2,[9,15,-10,-10]);
            C := MATRIX(2,2,[4,0,0,4]);
        else:
            error "Index out of range 1..7";
    end case;
    if ndx in [1,3,5] then
        return p, sub<GL(2,p) | A, B >;
    else
        return p, sub<GL(2,p) | A, B, C >;
    end if;
end function;

intrinsic ZASSENHAUSNEARFIELD(n :: RNGINTELT) -> NFDZSS
{Create the irregular nearfield number n)}
    requirerange n, 1, 7;
    p, S := irrNF(n);
    K := GF(p,2);
    E, φ := VECTORSPACE(K, PRIMEFIELD(K));
```

The associative array $\mu$ maps field elements to matrices.

```
    μ := ASSOCIATIVEARRAY(E);
    ω := φ(K ! 1);
    for x in S do μ[ω*x] := x; end for;
```

Create a new nearfield object and assign its attributes.

```
    NF := NEW(NFDZSS);
    NF`ndx := n;
    NF`p := p;
    NF`q := p;
```

```
    NF`gf := K;
    NF`prim := PrimitiveElement(K);
    NF`sz := p;
    NF`φ := φ;
    NF`μ := μ;
    NF`matgrp := S;
    NF`ψ := map< S → NF | x ↦ (ω*x)@@φ, y ↦ μ[φ(y`elt)] >;
    return NF;
end intrinsic;
```

## 3.4 Nearfield arithmetic

### 3.4.1 Addition

First define a few functions which will be internal to the package file. The mutation operators are not strictly necessary because the default options in the package file `System/mutate.m` will be used if no intrinsic is provided for objects of type NfdElt.

```
sameNF := "Elements must belong to the same nearfield";
procedure op_mutate(~x, ~y, op) op(~x`elt, ~y`elt); end procedure;
```

The operations of addition, subtraction and negation are inherited from the underlying Galois field and therefore they are quite straightforward to implement.

```
intrinsic '+' (x :: NfdElt, y :: NfdElt) → NfdElt
{ x + y }
    require x`parent eq y`parent: sameNF;
    return Element(x`parent, x`elt+y`elt);
end intrinsic;

intrinsic '+:=' (~x :: NfdElt, ~y :: NfdElt)
{ x +:= y }
    require x`parent eq y`parent: sameNF;
    op_mutate(~x, ~y, '+:=');
end intrinsic;

intrinsic '-' (x :: NfdElt, y :: NfdElt) → NfdElt
{ x - y }
    require x`parent eq y`parent: sameNF;
    return Element(x`parent, x`elt-y`elt);
end intrinsic;

intrinsic '-' (x :: NfdElt) → NfdElt
{ -x }
    return Element(x`parent, -x`elt);
end intrinsic;

intrinsic '-:=' (~x :: NfdElt, ~y :: NfdElt)
{ x +:= y }
    require x`parent eq y`parent: sameNF;
```

```
    op_mutate(~x, ~y, '-:=');
end intrinsic;
```

### 3.4.2 Multiplication

The operation of multiplication distinguishes a nearfield from a field. In a nearfield, multiplication is not commutative and the left distributive law fails.

```
intrinsic '*' (n :: RngIntElt, y :: NfdElt) -> NfdElt
{Left scalar multiple of a nearfield element y}
    N := y`parent;
    m := n mod N`p;
    return Element(N, m*y`elt);
end intrinsic;

intrinsic '*' (x :: NfdElt, n :: RngIntElt) -> NfdElt
{Right scalar multiple of a nearfield element x}
    N := x`parent;
    m := n mod N`p;
    return Element(N, m*x`elt);
end intrinsic;

intrinsic '*:=' (~x :: NfdElt, ~y :: NfdElt)
{x *:= y}
    require x`parent eq y`parent: sameNF;
    op_mutate(~x, ~y, '*:=');
end intrinsic;
```

In order to define the multiplication in a Dickson nearfield we begin with a Dickson triple $(p, h, v)$ and a primitive element $\zeta$ of the Galois field $K = \mathrm{GF}(q^v)$, where $q = p^h$.

**Lemma 3.3** ([38, Lemma 6.3.2])**.** *If $(p, h, v)$ is a Dickson triple and $q = p^h$, then*

$$1, \frac{q^2-1}{q-1}, \frac{q^3-1}{q-1}, \ldots, \frac{q^v-1}{q-1}$$

*is a complete residue system modulo $v$. In particular, $(q^v - 1)/(q - 1) \equiv 0 \mod v$.*

Adapting the approach of [23] to our situation (as in [21, p. 237]) we deduce from this lemma that $A = \langle \zeta^v \rangle$ is a group of order $m = (q^v - 1)/v$ and the elements $s_i = \zeta^{(q^i-1)/(q-1)}$ $(1 \le i \le v)$ are coset representatives for $A$ in $K^\times$. Let $\Phi$ denote the Frobenius automorphism $x \mapsto x^q$ of $K$ and define $\rho : K^\times \to \mathrm{Gal}(K/\mathrm{GF}(p))$ by $\rho(u) = \Phi^i$ if $u \in s_i A$; that is, letting automorphisms of $K$ act on the right, we have $x^{\rho(u)} = x^{q^i}$. The map $\rho$ is not a homomorphism. However, its image is the cyclic group of order $v$ generated by $\Phi = \rho(\zeta)$ and the fixed field of $\operatorname{im}\rho$ is $\mathrm{GF}(q)$; thus $\operatorname{im}\rho$ may be identified with $\mathrm{Gal}(K/\mathrm{GF}(q))$.

**Lemma 3.4.** *For all $u, w \in K^\times$ we have $\rho(w)\rho(u) = \rho(w^{\rho(u)}u)$.*

*Proof.* We may suppose that $\rho(u) = \Phi^i$ and $\rho(w) = \Phi^j$ for some $i$ and $j$. Then $u = s_i a$ and $w = s_j b$ for some $a, b \in A$. Thus $uw^{\rho(u)} = s_i s_j^{\Phi^i} a b^{\Phi^i} \in s_i s_j^{\Phi^i} A$. Furthermore, $s_i s_j^{\Phi^i}$ is $\zeta$ raised to the power

$$\frac{q^i - 1}{q - 1} + \left(\frac{q^j - 1}{q - 1}\right) q^i = \frac{q^{i+j} - 1}{q - 1}$$

and so $s_i s_j^{\Phi^i} A = s_{i+j} A$. Thus $\rho(w^{\rho(u)}u) = \Phi^{i+j} = \rho(w)\rho(u)$. □

**Definition 3.5.** Given a Dickson triple $(p, h, v)$ and a primitive element $\zeta$ of the Galois field $K = GF(q^v)$, where $q = p^v$, the *Dickson nearfield* $D(p, h, v, \zeta)$ is the set $K$ with addition as in $K$, $0 \circ w = w \circ 0 = 0$, and multiplication in $K^\times$ defined by $w \circ u = w^{\rho(u)}u$.

It follows from Lemma 3.4 that $\rho(w \circ u) = \rho(w)\rho(u)$ for all $w, u \in K^\times$. To see that $D(p, h, v, \zeta)$ is a nearfield we check the associative and the right distributive laws. The associative law obviously holds if any factor is 0, otherwise we have:

$$(w \circ u) \circ x = (w^{\rho(u)}u) \circ x = (w^{\rho(u)}u)^{\rho(x)}x = w^{\rho(u \circ x)}(u \circ x) = w \circ (u \circ x).$$

Similarly, if any one of $w$, $u$, $x$ or $w+u$ is 0, it follows directly that $(w+u) \circ x = w \circ x + u \circ x$, otherwise:

$$(w + u) \circ x = (w + u)^{\rho(x)}x = w^{\rho(x)}x + u^{\rho(x)}x = w \circ x + u \circ x.$$

The function reg_mult implements multiplication in a Dickson nearfield.

```
reg_mult := function(N, w, u)
   v := N`v;
   if v eq 1 then return w*u; end if;
   q := N`q;
   s := LOG(N`prim, u) mod N`v;
   e := N`ρ[s+1];
   return w^e*u;
end function;
```

To define multiplication between non-zero elements in an irregular nearfield, the elements are mapped to matrices in the group of units, the matrices are multiplied and the result is pulled back to the nearfield.

```
irreg_mult := function(N, w, u);
   φ := N`φ;
   A := N`μ[φ(w)];
   B := N`μ[φ(u)];
   return (φ(N`gf ! 1)*A*B)@@φ;
end function;

intrinsic '*' (x :: NFDELT, y :: NFDELT) → NFDELT
{ x * y }
   require x`parent eq y`parent: sameNF;
   N := x`parent;
   K := N`gf;
   w := x`elt;
   u := y`elt;
   if ISZERO(w) or ISZERO(u) then return ZERO(N); end if;
   if ISONE(w) then return y; end if;
   if ISONE(u) then return x; end if;
   pr := NEW(NFDELT);
   pr`parent := N;
   pr`elt := TYPE(N) eq NFDDCK select reg_mult(N, w, u) else irreg_mult(N, w, u);
```

**return** *pr* ;
**end intrinsic**;

Before moving on to the implementation of inverses we deduce a little more from the calculations which preceded the definition of a Dickson nearfield. A version of these calculations first appeared in [23].

We retain the notation introduced earlier in this section. In particular, if $D$ denotes the Dickson nearfield constructed from $K = \mathrm{GF}(q^v)$ as above, then $\rho : D^\times \to \mathrm{Gal}(K/\mathrm{GF}(p))$ is a homomorphism whose kernel is the set $A = \langle \zeta^v \rangle$. Thus $A$ is both a subgroup of the group of units of $K$ and a subgroup of the group of units of $D$. Furthermore, for $a \in A$ and $w \in D$ we have $w \circ a = w^{\rho(a)}a = wa$.

It follows that $A$ is a cyclic subgroup of $D^\times$ and the sets $s_i \circ A = s_i A$ are the cosets of $A$ in $D^\times$ and also the cosets of $A$ in $K^\times$. If $u \in s_i A$, it follows from the definition of the product that $u^{[k]} = u^{(q^{ki}-1)/(q-1)}$, where the notation $[v]$ indicates that the power is to be computed in $D$. In particular, $\zeta^{[k]} = s_k$ and so $D^\times/A$ is a cyclic group generated by $\zeta A$, hence $D^\times$ is metacyclic. If $u \in A$, then $u^{[k]} = u^k$.

Setting $m = (q^v - 1)/v$ and $t = m/(q-1)$ we see that $\zeta^{[v]} = \zeta^{(q^v-1)/(q-1)} = (\zeta^v)^t$.

**Lemma 3.6.** *$w^{[-1]} \circ a \circ w = a^{\rho(w)}$ for all $w \in D^\times$ and all $a \in A$.*

*Proof.* We have

$$\begin{aligned} w^{[-1]} \circ a \circ w &= (w^{[-1]}a) \circ w = (w^{[-1]}a)^{\rho(w)}w = (w^{[-1]})^{\rho(w)}a^{\rho(w)}w \\ &= (w^{[-1]})^{\rho(w)}wa^{\rho(w)} = (w^{[-1]} \circ w)a^{\rho(w)} = a^{\rho(w)}. \end{aligned}$$

□

**Lemma 3.7.** *The centre $\mathcal{Z}(D)$ of $D$ is isomorphic to the Galois field GF(q) and the group of units of $\mathcal{Z}(D)$ is contained in $A$.*

*Proof.* By the previous lemma the subgroup $E = \{a \in A \mid a^q = a\}$ is contained in $\mathcal{Z}(D)$ and it is clear that $E \cup \{0\}$ is $\mathrm{GF}(q)$.

Conversely, if $w$ is a non-zero element of $\mathcal{Z}(D)$, then we may write $w = s_i a'$ for some $i$ and some $a' \in A$. Then for all $a \in A$ we have $a = w^{[-1]} \circ a \circ w = a^{\rho(w)}$ and thus $A$ is contained in the fixed field of $\Phi^i$. It follows that $(q^v - 1)/v$ divides $q^i - 1$ and $q^i - 1$ divides $q^v - 1$. Using the fact that every prime divisor of $v$ divides $q - 1$ a rather lengthy calculation (see [38, p. 6.24]) shows that $i = v$; that is, $w \in A$. Now $w = \zeta^{[-1]} \circ w \circ \zeta = w^q$ and therefore $w \in E$, as required. □

**Theorem 3.8.** *If $(p, h, v)$ is a Dickson triple, $q = p^h$, $m = (q^v - 1)/v$, $t = m/(q-1)$ and if $\zeta$ is a primitive element of GF($q^v$), there is an isomorphism $\varphi$ from the group with generators $a$ and $b$ and relations*

$$a^m = 1, \quad b^v = a^t, \quad b^{-1}ab = a^q.$$

*to the group of units of the Dickson nearfield $D(p, h, v, \zeta)$ such that $\varphi(a) = \zeta^v$ and $\varphi(b) = \zeta$. The inverse of $\varphi$ is given by $\varphi^{-1}(\zeta^s) = b^i a^j$, where $i$ is the unique integer $(1 \le i \le v)$ such that $(q^i - 1)/(q-1) \equiv s \mod v$ and $j = ((q^i - 1)/(q-1) - s)/v$.*

*Proof.* We have already shown that $\zeta^v$ and $\zeta$ satisfy the given relations. Conversely, it is clear that the group defined by the given relations has order $mv = q^v - 1$. The formula $\varphi^{-1}(\zeta^s) = b^i a^j$ follows from the fact that $\zeta^s \in s_i A = s_i \circ A$. □

### 3.4.3 Inverses, conjugates, powers

```
reg_inv := function(N, x)
    v := N`v;
    if v eq 1 then return x`elt^-1; end if;
    q := N`q;
    z := N`prim;
    s := Log(z, x`elt);
    e := N`ρ[s mod v + 1];
    r := Solution(e, -s, q^v-1);
    return z^r;
end function;

irreg_inv := function(N, x)
    φ := N`φ;
    A := N`μ[φ(x`elt)];
    return (φ(N`gf ! 1)*A^-1)@@φ;
end function;

intrinsic Inverse(x :: NfdElt) → NfdElt
{ x^-1 }
    require not IsZero(x): "Cannot invert the zero element";
    N := x`parent;
    inv := New(NfdElt);
    inv`parent := N;
    inv`elt := Type(N) eq NfdDck select reg_inv(N, x) else irreg_inv(N, x);
    return inv;
end intrinsic;

intrinsic '/' (x :: NfdElt, y :: NfdElt) → NfdElt
{ The quotient x/y of nearfield elements x and y }
    require x`parent eq y`parent: sameNF;
    return x*Inverse(y);
end intrinsic;

intrinsic '^' (x :: NfdElt, n :: RngIntElt) → NfdElt
{ The n-th power of nearfield element x }
    t := Identity(x`parent);
    if n lt 0 then x := Inverse(x); n := -n; end if;
    while n gt 0 do
        if IsOdd(n) then
            t *:= x;
            if n eq 1 then break; end if;
        end if;
        x *:= x;
        n := n div 2;
    end while;
    return t;
```

```
end intrinsic;

intrinsic '^' (x :: NfdElt, y :: NfdElt) → NfdElt
{The conjugate of x by y}
  return Inverse(y)*x*y;
end intrinsic;
```

### 3.5 Operations on nearfields

By defining a PrintNamed intrinsic we link into Magma's printing services so that simply typing the name of a nearfield will print the object. This is one of the intrinsics (or a variant, such as Print) which should always be defined for a new type.

```
intrinsic PrintNamed(N :: NfdDck, level :: MonStgElt, name :: MonStgElt)
{Print description of the nearfield N}
  msg :=
    Sprintf("Nearfield %o of Dickson type defined by the pair",
    name);
  if level eq "Minimal" then
    printf msg * " (%o, %o)", N`q, N`v;
  elif level eq "Magma" then
    printf "DicksonNearfield(%o,%o)", N`q,N`v;
  else
    printf msg * " (%o, %o)\nOrder = %o", N`q ,N`v,#N;
  end if;
end intrinsic;

intrinsic PrintNamed(N :: NfdZss, level :: MonStgElt, name :: MonStgElt)
{Print description of the nearfield N}
  msg :=
    Sprintf("Irregular nearfield %o with Zassenhaus number",
    name);
  if level eq "Minimal" then
    printf msg * " %o", N`ndx;
  elif level eq "Magma" then
    printf "ZassenhausNearfield(%o)", N`ndx;
  else
    printf msg * " %o\nOrder = %o", N`ndx, #N;
  end if;
end intrinsic;
```

Tests for equality of nearfields will be given in §4.

```
intrinsic '#' (N :: Nfd) → RngIntElt
{Cardinality of the nearfield N}
  return #(N`gf);
end intrinsic;

intrinsic Cardinality(N :: Nfd) → RngIntElt
{Cardinality of the nearfield N}
```

```
  return #(N`gf);
end intrinsic;
```

### 3.6 Operations on elements

Because the element type NfdElt has been declared, a Parent intrinsic must be defined and it must return an object of type Nfd.

```
intrinsic Parent(x :: NfdElt) -> Nfd
{Return the parent of the nearfield element x}
  return x`parent;
end intrinsic;

intrinsic Print(x :: NfdElt)
{Print a nearfield element x}
  printf "%o", x`elt;
end intrinsic;
```

Defining the Hash intrinsic considerably speeds up the set and sequence machinery.

```
intrinsic Hash(x :: NfdElt) -> RngIntElt
{Return the hash value for a nearfield element x}
  return Hash(Parent(x)`gf);
end intrinsic;

intrinsic '!' (N :: Nfd, x :: FldFinElt) -> NfdElt
{Coerce a finite field element x into the nearfield N}
  return Element(N, x);
end intrinsic;

intrinsic Element(N :: Nfd, x :: FldFinElt) -> NfdElt
{Create a nearfield element from a finite field element}
  flag, y := IsCoercible(N`gf, x);
  require flag: "Finite field element is not in the carrier" *
    " set of the nearfield";
  X := New(NfdElt);
  X`parent := N;
  X`elt := y;
  return X;
end intrinsic;
```

The functions IsCoercible and '*in*' are standard intrinsics which should be defined for a new type. The following versions apply to both NfdDck and NfdZss types.

```
intrinsic IsCoercible(N :: Nfd, x :: Any) -> BoolElt, Any
{True iff the finite field element x is coercible
 into the nearfield N}
  M := Parent(x);
  if Type(M) eq Type(N) and M eq N then
    return true, x;
  end if;
```

```
   flag, y := IsCoercible(N`gf, x);
   if flag then
      return true, Element(N, y);
   else
      return false, "Illegal coercion";;
   end if;
end intrinsic;

intrinsic ElementToSequence(x :: NfdElt) -> []
{Create a sequence from an element x of a nearfield}
      return ElementToSequence(x`elt);
 end intrinsic;

intrinsic 'in'(x :: Any, N :: Nfd) -> BoolElt
{True iff the element x is in the nearfield N}
   M := Parent(x);
   return Type(M) eq Type(N) and M eq N;
end intrinsic;

intrinsic Random(N :: Nfd) -> NfdElt
{Create a random element of the nearfield N}
   X := New(NfdElt);
   X`parent := N;
   X`elt := Random(N`gf);
   return X;
end intrinsic;

intrinsic Identity(N :: Nfd) -> NfdElt
{Create the multiplicative identity of the nearfield N}
   X := New(NfdElt);
   X`parent := N;
   X`elt := (N`gf) ! 1;
   return X;
end intrinsic;

intrinsic Zero(N :: Nfd) -> NfdElt
{Create the additive identity of the nearfield N}
   X := New(NfdElt);
   X`parent := N;
   X`elt := (N`gf) ! 0;
   return X;
end intrinsic;

intrinsic IsZero(x :: NfdElt) -> BoolElt
{True if x is the additive identity of the nearfield N}
   return x`elt eq (x`parent`gf) ! 0;
end intrinsic;

intrinsic IsIdentity(x :: NfdElt) -> BoolElt
```

```
{True if x is the multiplicative identity of the nearfield N}
  return x`elt eq (x`parent`gf) ! 1;
end intrinsic;

intrinsic 'eq' (x :: NfdElt, y :: NfdElt) -> BoolElt
{x eq y}
  require x`parent eq y`parent: sameNF;
  return x`elt eq y`elt;
end intrinsic;

intrinsic 'ne' (x :: NfdElt, y :: NfdElt) -> BoolElt
{x ne y}
  require x`parent eq y`parent: sameNF;
  return x`elt ne y`elt;
end intrinsic;
```

### 3.7 The group of units

```
intrinsic IsUnit(x :: NfdElt) -> BoolElt
{True if the nearfield element x is a unit}
  return x`elt ne (x`parent`gf) ! 0;
end intrinsic;
```

If $N$ is a nearfield and $F = \mathcal{K}(N)$ is its kernel, $N$ is a vector space over $F$ and for all $u \in N^\times$, the map $x \mapsto x \circ u$ is an $F$-linear transformation. This action of $N^\times$ on the non-zero elements of the vector space is transitive and fixed-point-free. (See §3.8 for a proof that the kernel is $\mathrm{GF}(q)$.)

Similarly, we may regard $N$ as a vector space over its prime field and again the elements of $N^\times$ act as linear transformations. In the following code the vector space $E$ could be either a vector space over the kernel or a vector space of the prime field. The default setting is to use the kernel. But if the parameter *LargeMatrices* is set to true when a regular nearfield is first defined, the prime field will be used. For irregular nearfields the kernel coincides with the prime field.

```
matrixUnitGroup := function(N)
  K := N`gf;
  z := K.1;
  v := N`v;
  φ := N`φ;
  ζ := N`prim;
  E := Image(φ);
  n := Dimension(E);
  F<x> := BaseRing(E);
  basis := [Element(N, z^i) : i in [0..n-1]];
  a := Element(N, ζ^v);
  A := Matrix(F, n, n, [φ((x*a)`elt) : x in basis]);
  b := Element(N, ζ);
  B := Matrix(F, n, n, [φ((x*b)`elt) : x in basis]);
```

```
    G := sub< GL(E) | A, B >;
    G`Order := #N-1;
```

In addition to the matrix group $G$ we want an embedding $\psi : G \to N$ and its inverse, which is defined only on the non-zero elements of $N$.

```
    q := N`q;
    psi_inv := function(y)
      s := Log(ζ, y`elt);
      t := s mod v + 1;
      i := N`twist[t];
      e := N`ρ[t];
      j := (s - (e-1) div (q-1)) div v;
      return B^i*A^j;
    end function;
    ω := φ(K ! 1);
    ψ := map< G -> N | x :-> (ω*x)@@φ, y :-> psi_inv(y) >;
    return G, ψ;
  end function;
```

Theorem 3.8 shows that the group $U$ of units of the Dickson nearfield $D = D(p, h, v, \zeta)$ has generators $a$ and $b$ and relations $a^m = 1$, $b^v = a^t$ and $b^{-1}ab = a^q$, where $q = p^h$, $m = (q^v-1)/v$ and $t = m/(q-1)$. Furthermore, Ellers and Karzel [23] show that $\gcd(v, t) = \gcd(q-1, t) \leq 2$. Equality holds if and only if $v \equiv 2 \mod 4$ and $q \equiv 3 \mod 4$ and this in turn is equivalent to the Sylow 2-subgroup of $U$ being a generalised quaternion group.

The centre of $D$ is $\mathrm{GF}(q)$ and its group of units is generated by $\zeta^{vt}$.

```
  intrinsic UnitGroup(N :: Nfd) -> GrpMat, Map
  {The unit group of the nearfield N returned as
   a matrix group M and a map from M to N}
    if not assigned N`matgrp then
      U, ψ := matrixUnitGroup(N);
      N`matgrp := U;
      N`ψ := ψ;
    end if;
    return N`matgrp, N`ψ;
  end intrinsic;

  intrinsic UnitGroup(`GrpPerm, N :: Nfd) -> GrpPerm
  {The unit group of the nearfield N returned as
   a permutation group}
    U := UnitGroup(N);
    require #U le 10^8 : "Unit group is too large to construct as a
    permutation group";
    _, H, _ := CosetAction(U, sub<U|>);
    return H;
  end intrinsic;

  intrinsic UnitGroup(`GrpPC, N :: NfdDck) -> GrpPC
  {The unit group of the nearfield N returned as a PC-group}
```

```
    U := UnitGroup(N);
    LMGInitialise(U);
    _, pcg, _ := LMGSolubleRadical(U);
    return pcg;
end intrinsic;

intrinsic UnitGroup(`GrpPC, N :: NfdZss) -> GrpPC
{The unit group of the nearfield N returned as a PC-group}
    require N`ndx in [1..4]: "Unit group not soluble";
    U := UnitGroup(N);
    LMGInitialise(U);
    _, pcg, _ := LMGSolubleRadical(U);
    return pcg;
end intrinsic;

intrinsic Order(x :: NfdElt) -> RngIntElt
{Order of the unit x of a nearfield}
    require IsUnit(x): "Attempting to find the order of a non-unit";
    N := x`parent;
    one := Identity(N);
    if x eq one then return 1; end if;
    n := #N-1;
    ord := 1;
    facts := Factorisation(n);
    for term in facts do
        p, e := Explode(term);
        y := x^(n div p^e);
        f := 0;
        while y ne one do
            y := y^p;
            f +:= 1;
        end while;
        ord *:= p^f;
    end for;
    return ord;
end intrinsic;
```

As a matrix group, the unit group $U$ acts regularly on the non-zero vectors of the underlying vector space $E$ and consequently the affine group $E \cdot U$ is sharply two-transitive. As shown in §2.1, all sharply two-transitive groups occur in this way.

```
intrinsic AffineGroup(N :: Nfd) -> GrpMat
{The sharply two-transitive affine group associated with a
 nearfield, returned as a matrix group}
    U := UnitGroup(N);
    F := BaseRing(U);
    one := Matrix(F, 1, 1, [1]);
    gens := [DiagonalJoin(U.i, one) : i in [1..NGens(U)]];
```

```
    n := Dimension(U);
    C := DiagonalJoin(U ! 1, one);
    C[n+1, 1] := 1;
    Append(~gens, C);
    G := sub<GL(n+1, F) | gens >;
    G`Order := #N*(#N-1);
    return G;
end intrinsic;
```

To convert from a matrix group to a permutation group we construct the permutation representation on the cosets of the unit group. Given that the affine group has $n$ generators, the following code relies on the assumption that the unit group of the nearfield is generated by the first $n-1$ generators.

```
intrinsic AffineGroup(`GrpPerm, N :: Nfd) -> GrpPerm
{The sharply two-transitive affine group associated with a
 nearfield, returned as a permutation group}
    G := AffineGroup(N);
    S := sub<G | [G.i : i in [1..Ngens(G)-1]] >;
    require Index(G, S) le 10^7 :
                "Degree of permutation group is too large";
    _, H, _ := CosetAction(G, S);
    H`Order := #N*(#N-1);
    return H;
end intrinsic;

intrinsic AffineGroup(`GrpPC, N :: NfdDck) -> GrpPC
{The sharply two-transitive affine group associated with a
 regular nearfield, returned as a PC-group}
    A := AffineGroup(N);
    LMGInitialise(A);
    _, pcg, _ := LMGSolubleRadical(A);
    return pcg;
end intrinsic;

intrinsic AffineGroup(`GrpPC, N :: NfdZss) -> GrpPC
{The sharply two-transitive affine group associated with an
 irregular nearfield, returned as a PC-group}
    require N`ndx in [1..4]: "Unit group not soluble";
    A := AffineGroup(N);
    LMGInitialise(A);
    _, pcg, _ := LMGSolubleRadical(A);
    return pcg;
end intrinsic;
```

### 3.8 Miscellaneous

```
intrinsic PrimeField(N :: Nfd) -> FldFin
{Return the prime field of the nearfield N}
```

```
  return GF(N`p);
end intrinsic;
```

**Lemma 3.9.** *If $(p, h, v)$ is a Dickson triple and if $\zeta$ is a primitive element of $K = GF(q^v)$, where $q = p^h$, then every element of $K$ can be written as a polynomial in $\zeta^v$ with coefficients in $GF(q)$.*

*Proof.* (Zassenhaus [67, p. 190]) Let $F$ be the subfield of $K$ generated by $\zeta^v$. Then $F = \mathrm{GF}(q^\ell)$ for some divisor $\ell$ of $v$. The order of $\zeta^v$ is $(q^v - 1)/v$ and therefore $(q^v - 1)/v$ divides $q^\ell - 1$. But $q^{v/2} + 1 \geq 2^{v/2} + 1 > v$ and so $\ell = v$ and hence $F = K$. □

**Corollary 3.10.** *The kernel of $D = D(p, h, v, \zeta)$ is $GF(q)$.*

*Proof.* If $A = \langle \zeta^v \rangle$, then for $w \in D$ and $a \in A$ we have $w \circ a = wa$. From the Lemma, $\zeta = f(\zeta^v)$ for some $f(x) \in \mathrm{GF}(q)[x]$. Therefore, if $w \in \mathcal{K}(D)$, $w \circ \zeta = w\zeta$, whence $w^q = w$. Thus $\mathcal{K}(D) \subseteq \mathrm{GF}(q)$. The converse is clear and so $\mathcal{K}(D) = \mathrm{GF}(q) = \mathcal{Z}(D)$. □

For the irregular nearfields it is clear that the kernel is the prime field.

```
intrinsic Kernel(N :: Nfd) -> FldFin
{Return the kernel of the nearfield N as a finite field}
  return GF(N`q);
end intrinsic;
```

# 4 Complements and 1-cocycles

If $\Gamma = \mathrm{Gal}(K/\mathrm{GF}(p))$ and $S = \Gamma \ltimes K^\times$ is the semidirect product of $\Gamma$ and $K^\times$, it follows from Lemma 3.4 that $D^\times \to S : w \mapsto \rho(w)w$ is an embedding of the multiplicative group $D^\times$ of $D(p, h, v, \zeta)$ in $S$, where multiplication in $S$ is defined by

$$(\gamma_1 a_1)(\gamma_2 a_2) = \gamma_1\gamma_2 a_1^{\gamma_2} a_2.$$

If $U$ is the image of $D^\times$ in $S$, then $\Gamma \cap U = 1$, $\Gamma U = S$ and $K^\times \cap U = A = \langle \zeta^v \rangle$. In fact, from the definition of $\rho$, we have $UK^\times = \Gamma_0 \ltimes K^\times$, where $\Gamma_0 = \mathrm{Gal}(K/\mathrm{GF}(q))$.

```
intrinsic ExtendedUnitGroup(N :: NfdDck) -> GrpMat
{The extended unit group of a Dickson nearfield}
  U, _ := UnitGroup(N);
  z := (N`gf).1;
  q := N`q;
  phi := N`phi;
  n := Dimension(U);
  C := Matrix(n, n, [phi(z^(q*i)) : i in [0..n-1]]);
  G := sub< GL(n, BaseRing(U)) | U, C >;
  G`Order := Order(U)*N`v;
  return G;
end intrinsic;
```

In the remainder of this section we reverse the above process and describe how to construct a Dickson nearfield from a complement of $\Gamma$ in $\Gamma \ltimes K^\times$. This will lead to an efficient criterion

for isomorphism testing of nearfields including a simple construction for the isomorphism itself.

Therefore, suppose that $K = \mathrm{GF}(p^n)$, $\Gamma = \mathrm{Gal}(K/\mathrm{GF}(p))$ and that $U$ is a subgroup of $S = \Gamma \ltimes K^\times$ such that $\Gamma \cap U = 1$ and $\Gamma U = S$.

For all $u \in U$ there are unique elements $\xi(u) \in \Gamma$ and $\theta(u) \in K^\times$ such that

$$u = \xi(u)\theta(u). \tag{1}$$

It follows from (1) that

$$\xi(wu) = \xi(w)\xi(u), \quad \text{and} \tag{2}$$

$$\theta(wu) = \theta(w)^{\xi(u)}\theta(u). \tag{3}$$

The map $\xi : U \to \Gamma$ is a homomorphism and since $\Gamma$ is cyclic and generated by $x \mapsto x^p$, the image $\Gamma_0$ of $\xi$ is cyclic and generated by $\Phi$, where $\Phi(x) = x^{p^h}$ for some $h$. If $q = p^h$, the fixed field of $\Phi$ is $\mathrm{GF}(q)$ and thus $\Gamma_0 = \mathrm{Gal}(K/\mathrm{GF}(q))$. Then $n = hv$, where $v = |\Gamma_0|$. We have $U \subseteq S_0 = \Gamma_0 \ltimes K^\times$, $\Gamma_0 \cap U = 1$ and $S_0 = \Gamma_0 U = K^\times U$.

**Lemma 4.1.** *$\theta : U \to K^\times$ is a bijection and a 1-cocycle.*

*Proof.* Suppose that $\theta(w) = \theta(u)$. Then $\xi(u)\xi(w)^{-1} = uw^{-1} \in \Gamma \cap U = 1$ and hence $w = u$. Thus $\theta$ is one-to-one and since $|U| = |K^\times|$, it is a bijection. Equation (3) shows that $\theta$ is a 1-cocycle. □

If $A = \ker \xi$, then $A = U \cap K^\times$ and $A$ is the unique subgroup of order $m = (q^v - 1)/v$ in $K^\times$. For all $a \in A$ we have $\theta(a) = a$. Thus for $u \in U$ and $a \in A$ we have $\theta(ua) = \theta(u)a$ and therefore $\theta$ induces a bijection $\bar{\theta} : U/A \to K^\times/A : \bar{u} \mapsto \theta(u)A$, where $\bar{u} = uA$. Similarly, $\xi$ induces a bijection $\bar{\xi} : U/A \to \Gamma_0$ and if $\sigma = \bar{\theta}\bar{\xi}^{-1}$, then from (3) we have

$$\sigma(\gamma_1\gamma_2) = \sigma(\gamma_1)^{\gamma_2}\sigma(\gamma_2) \tag{4}$$

and so $\sigma : \Gamma_0 \to K^\times/A$ is a 1-cocycle.

The proof of the next lemma is essentially the argument of [23, p. 253].

**Lemma 4.2.** *There exists a generator $\zeta$ of the cyclic group $K^\times$ such that $\Phi\zeta \in U$.*

*Proof.* Choose $\omega \in U$ such that $\xi(\omega) = \Phi$. If $\zeta$ is a primitive element of $K$, then $\theta(\omega) = \zeta^s$ for some $s$ and hence $\theta(\omega^i) = \zeta^{s(q^i-1)/(q-1)}$ for all $i$. The maps $\bar{\xi}$ and $\bar{\theta}$ are bijections and therefore the elements $\sigma_i = \zeta^{s(q^i-1)/(q-1)}$ $(0 \le i < v)$ are the coset representatives of $A$ in $K^\times$. That is, for $0 \le i < v$, the quantities $s(q^i-1)/(q-1) \mod v$ are distinct and $s(q^v-1)/(q-1) \equiv 0 \mod v$. Since $\gcd(s, v) = 1$, it follows that

$$\frac{q^i-1}{q-1} \not\equiv 0 \mod v \quad \text{for } 0 \le i < v \quad \text{and} \quad \frac{q^v-1}{q-1} \equiv 0 \mod v.$$

Let $m = (q^v-1)/v$ and let $m'$ be the product of the primes $r$ such that $r \mid m$ and $r \nmid s$. Then $\gcd(s + m'v, mv) = 1$. Let $\zeta' = \zeta^{s+m'v}$; then $\zeta'$ generates $K^\times$. Now $\zeta^{m'v} \in A$ and therefore $\theta(\omega\zeta^{m'v}) = \zeta'$ and $\xi(\omega\zeta^{m'v}) = \Phi$. Thus $\Phi\zeta' = \omega\zeta^{m'v} \in U$, as required. □

In the course of this proof we have shown that $v(q-1) \mid q^v - 1$. A number theoretic argument now shows that $(q, v)$ is a Dickson pair (see [38]).

### 4.1 Isomorphisms and automorphisms

We continue with the notation established above. That is, $U$ is a complement to $\Gamma_0$ in $S_0$ and $\zeta$ is a primitive element of $K$ such that $\Phi\zeta \in U$.

Since $(\Phi\zeta)^i = \Phi^i \zeta^{(q^i-1)/(q-1)}$, the subgroup $U$ is uniquely determined by the coset $\zeta A = \sigma(\Phi)$. Let $V$ be the (unique) subgroup of order $v$ in $K^\times$ and define $\lambda : K^\times \to V$ by $\lambda(b) = b^m$. Then $\lambda$ is a homomorphism onto $V$ with kernel $A$ and so $K^\times/A \simeq V$. It follows that $U$ is uniquely determined by the element $\delta = \zeta^m$ of order $v$. This provides a convenient test for equality.

```
intrinsic 'eq' (N :: NfdDck, M :: NfdDck) -> BoolElt
{N eq M}
  q := N`q;
  v := N`v;
  if q ne M`q or v ne M`v then return false; end if;
  m := (q^v-1) div v;
  return (N`prim)^m eq (M`prim)^m;
end intrinsic;

intrinsic 'eq' (N :: NfdZss, M :: NfdZss) -> BoolElt
{N eq M}
  return N`ndx eq M`ndx;
end intrinsic;

intrinsic 'ne' (N :: NfdDck, M :: NfdDck) -> BoolElt
{N ne M}
  q := N`q;
  v := N`v;
  if q ne M`q or v ne M`v then return true; end if;
  m := (q^v-1) div v;
  return (N`prim)^m ne (M`prim)^m;
end intrinsic;

intrinsic 'ne' (N :: NfdZss, M :: NfdZss) -> BoolElt
{N ne M}
  return N`ndx ne M`ndx;
end intrinsic;
```

We may identify the field $K$ with a vector space $E$ of dimension $v$ over $\mathrm{GF}(q)$. Given $\gamma \in \Gamma_0$ and $a \in K$, the map $e \mapsto e^\gamma a$ is a linear transformation of $E$, whence $S_0 \subseteq \mathrm{GL}(E)$. The affine group $U \ltimes E$ acts sharply doubly transitively on $E$ and it follows from Theorem 2.6 that $E$ can be given the structure of a nearfield with $U$ (isomorphic to) its group of units. In the notation of Theorem 2.6, $\Omega = E$, $M = K$, $\eta$ is the identity and $\mu = \theta^{-1}$.

If $a \circ b$ denotes the nearfield multiplication defined on $K^\times$ via this construction, then $\theta^{-1}(a \circ b) = \theta^{-1}(a)\theta^{-1}(b)$ and from (3) we have $a \circ b = a^{\rho(b)}b$, where $\rho = \xi\theta^{-1} : K^\times \to \Gamma_0$. If $b \in A$, then $\rho(ab) = \rho(a)$ and $\rho$ is completely determined by the induced map $\bar{\rho} = \sigma^{-1} : K^\times/A \to \Gamma_0$. Furthermore, for $w \in K^\times$ we have $\theta^{-1}(w) = \rho(w)w$ and so we recover the embedding defined in the first paragraph of this section.

**Theorem 4.3** ([23, Satz 4]). *If $q$ is a prime power and $D$ is a Dickson nearfield of order $q^v \neq 9$, centre $GF(q)$ and defining map $\rho : K^\times \to \Gamma_0$, then the cyclic normal subgroups of $D^\times$ are contained in $\ker\rho$. If $|D| = 9$, then $D^\times$ is a quaternion group and every element generates a cyclic normal subgroup.*

It follows from this theorem that if $U_1$ and $U_2$ are complements to $\Gamma_0$ in $S_0$, if $\varphi : U_1 \to U_2$ is an isomorphism and $|U_1| \neq 9$, then $\varphi$ preserves $A$. It then follows from Lemma 3.9 that $\varphi \in \mathrm{Gal}(K/\mathrm{GF}(p))$. If $\Phi\zeta_1 \in U_1$, where $\zeta_1$ generates $K^\times$, then $(\Phi\zeta_1)^\varphi = \Phi\zeta_2$, where $\zeta_2$ also generates $K^\times$. Setting $\delta_i = \zeta_i^m$ $(i = 1, 2)$ we have $\delta_1^\varphi = \delta_2$. Thus the nearfields corresponding to $U_1$ and $U_2$ are isomorphic if and only if the minimal polynomials of $\delta_1$ and $\delta_2$ are equal.

If $\phi$ is the Euler phi-function, there are $\phi(v)$ complements to $\Gamma_0$ in $S$ and if $g$ is the order of $p$ modulo $v$, there are $\phi(v)/g$ pairwise non-isomorphic Dickson nearfields of order $q^v$ with centre $\mathrm{GF}(q)$.

```
intrinsic IsIsomorphic(N1 :: NfdDck, N2 :: NfdDck) -> BoolElt, Map
{Test whether the regular nearfields N1 and N2 are
 isomorphic.  If they are, return an isomorphism}
  q := N1`q;
  v := N1`v;
  if q ne N2`q or v ne N2`v then
     return false, _;
  end if;
  m := (q^v - 1) div v;
  d1 := (N1`prim)^m;
  d2 := (N2`prim)^m;
  if MinimalPolynomial(d1) ne MinimalPolynomial(d2) then
     return false, _;
  end if;
  s := Log(d1, d2);
  _, t, _ := XGCD(s, q^v-1);
  return true, map< N1 -> N2 |
          x :-> Element(N2, ((x`elt)^s)), y :-> Element(N1, ((y`elt)^t)) >;
end intrinsic;
```

**Theorem 4.4.** *If $\Psi(x) = x^{p^g}$, the automorphism group of $D = D(p, h, v, \zeta)$ is the cyclic group $\langle\,\Psi\,\rangle$ of order $hv/g$ except for $D(3, 1, 2, \zeta)$ whose automorphism group is the symmetric group* $\mathrm{Sym}(3)$.

*Proof.* Suppose that $D \neq D(3, 1, 2, \zeta)$ and that $\varphi$ is an automorphism of $D$. By Theorem 4.3, $\varphi$ fixes $A$ and by Lemma 3.9, $\varphi \in \mathrm{Gal}(K/\mathrm{GF}(p))$. Thus $\varphi(x) = x^{p^\alpha}$ for some $\alpha$.

For $w, u \in K^\times$ we have

$$\varphi(w \circ u) = (w \circ u)^{p^\alpha} = (w^{p^\alpha})^{\rho(u^{p^\alpha})} u^{p^\alpha} \quad \text{and}$$
$$\varphi(w) \circ \varphi(u) = (w^{\rho(u)} u)^{p^\alpha} = w^{p^\alpha \rho(u)} u^{p^\alpha}$$

hence $\varphi(w)^{\rho(\varphi(u))} = \varphi(w)^{\rho(u)}$ for all $w$. It follows that $\rho(\varphi(u)) = \rho(u)$ for all $u$.

In particular, $\rho(\zeta) = \rho(\varphi(\zeta))$ and hence $\varphi(\zeta)\zeta^{-1} \in A$. It follows that $\zeta^{p^\alpha - 1} = p^{kv}$ for some $v$ and thus $p^\alpha - 1 \equiv kv \mod q^v - 1$. But $q^v - 1 \equiv 0 \mod v$ and so $p^\alpha - 1 \equiv 0 \mod v$. From this we deduce that $g$ divides $\alpha$ and hence $\varphi \in \langle\,\Psi\,\rangle$.

Conversely, suppose that $u \in \zeta^{(q^i-1)/(q-1)}A$. Then $\Psi(u) \in \zeta^{p^g(q^i-1)/(q-1)}A$. But $p^g \equiv 1 \bmod v$ and therefore $\zeta^{p^g}A = \zeta A$. Consequently $\rho(\Psi(u)) = \rho(u)$. We now have

$$\begin{aligned}\Psi(w \circ u) &= \Psi(w^{\rho(u)}u) = \Psi(w)^{\rho(u)}\Psi(u)\\ &= \Psi(w)^{\rho(\Psi(u))}\Psi(u)\\ &= \Psi(w) \circ \Psi(u)\end{aligned}$$

and therefore $\Psi$ is an automorphism of $D$. This completes the proof that $\mathrm{Aut}(D) = \langle \Psi \rangle$.

The group of units of $D(3, 1, 2, \zeta)$ is a quaternion group of order 8. If $\varphi$ is an automorphism which fixes the subgroup $A$ of order 4, then the argument just given shows that $\varphi$ is a field automorphism and hence its order is 1 or 2. The group of units has an automorphism of order 3 which permutes the three subgroups of order 4. It follows that the full automorphism group is Sym(3). □

TODO: Maps for Sym(3) and Zassenhaus nearfields

```
intrinsic AutomorphismGroup(N :: NfdDck) -> GrpPerm, Map
{The automorphism group A of the regular nearfield N and
 a map giving the action of A on N}
  if #N eq 9 then return Sym(3),_; end if;
  v := N`v;
  g := Order(ResidueClassRing(v) ! N`p);
  ord := v*N`h div g;
  A := CyclicGroup(ord);
  psi := map< car<A,N> -> N | pi :-> Element(N, (pi[2]`elt^(N`p^(g*alpha)))))
        where alpha is (1^pi[1]-1) mod ord >;
  return A, psi;
end intrinsic;
```

The following theorem is due to Foulser [25]. A proof can also be found in [27].

**Theorem 4.5.** *The automorphism group of a Zassenhaus nearfield is cyclic. Their orders are* 4, 2, 3, 1, 5, 2 *and* 1.

```
intrinsic AutomorphismGroup(N :: NfdZss) -> GrpPerm
{The automorphism group A of the irregular nearfield N and
 a map giving the action of A on N}
  order := [4, 2, 3, 1, 5, 2, 1];
  return CyclicGroup(order[N`ndx]);
end intrinsic;
```

# 5 Sub-nearfields

If $N$ is a Zassenhaus nearfield, its only proper sub-nearfield is its prime field, which is not of type NfdZss. Therefore the current implementation of ***sub***< for user types is unable to return this object and so for now we ignore them.

**Lemma 5.1** (Dancs [27, Lemma 6.1])**.** *If $(q, v)$ is a Dickson pair and $(q^i - 1)/(q - 1) \equiv j \bmod v$, then $\gcd(j, v) = \gcd(i, v)$.*

*Proof.* If $\xi = \gcd(j, v)$ and $\eta = \gcd(i, v)$, then $(q, \xi)$ and $(q, \eta)$ are Dickson pairs. Therefore $(q^i - 1)/(q - 1) \equiv 0 \mod \xi$ whence $\xi \mid i$ and so $\xi \mid \eta$. We have $\eta \mid i$ and consequently $(q^i - 1)/(q - 1) \equiv 0 \mod \eta$, whence $\eta \mid j$. It follows that $\eta \mid \xi$ and hence $\eta = \xi$. □

**Lemma 5.2** (Dancs [27, Lemma 6.2])**.** *If $(q, v)$ is a Dickson pair and if $t$ divides $v$, then $(q^v - 1)/(q^t - 1) \equiv v/t \mod v$.*

**Theorem 5.3** (Dancs [11, 12, 27])**.** *If $D = D(p, h, v, \zeta)$ is the Dickson nearfield based on the Galois field $K = GF(p^{hv})$, then for each divisor $\lambda$ of $hv$, $D$ contains exactly one sub-nearfield of order $p^\lambda$, namely $D(p, k, \lambda/k, \zeta^I)$, where $k = \gcd(hI, \lambda)$ and where $I = (p^{hv} - 1)/(p^\lambda - 1)$.*

*Proof.* Let $\rho : K^\times \to \mathrm{Gal}(K/\mathrm{GF}(p))$ be the map defined in §3.4.2 and let $\Phi = \rho(\zeta)$. If $F$ is the subfield of $K$ of size $p^\lambda$, then $w \circ u = w^{\rho(u)}u \in F$ for all $w, u \in F$, because $F$ is fixed by $\Phi$.

Then $\kappa = \zeta^I$ is a primitive element of $F$ and $\rho(\kappa) = \Phi^\alpha$, where $\alpha$ is the unique integer such that $0 \le \alpha < v$ and $\kappa \in \zeta^{(q^\alpha - 1)/(q-1)}A$, where $A = \langle \zeta^v \rangle$. It follows that $I \equiv (q^\alpha - 1)/(q - 1) \mod v$ and therefore, by Lemma 5.1, we have $\gcd(I, v) = \gcd(\alpha, v)$.

The fixed field of $\rho(\kappa)$ is $\mathrm{GF}(p^k)$ for some $k$ and since for all $x \in F$ we have $\rho(\kappa)(x) = x^{p^{h\alpha}}$, it follows that $k = \gcd(h\alpha, \lambda)$.

If $\beta \mid \gcd(hI, \lambda)$, then $\beta \mid \gcd(hI, hv) = h \gcd(I, v) = \gcd(\alpha, v)$ and so $\beta \mid h\alpha, \lambda$, whence $\beta \mid \gcd(h\alpha, \lambda) = k$. Similarly, if $\beta \mid \gcd(h\alpha, k)$, then $\beta \mid \gcd(hI, \lambda)$. Thus $k = \gcd(hI, \lambda)$ and $F$ is the underlying Galois field of the nearfield $D(p, k, \lambda/k, \zeta^I)$. □

```
intrinsic SubConstr(N :: NfdDck, E :: SeqEnum) -> NfdDck, Map
{The sub-nearfield of the Dickson nearfield N generated by E}
  if #E gt 0 and (Type(E[1]) ne NfdElt or E[1]`parent ne N) then
    return "elements on RHS must be in the nearfield", _;
  end if;
  v := N`v;
  h := N`h;
  L, g := sub< N`gf | [e`elt : e in E] >;
  _, p, λ := IsPrimePower(#L);
  I := (#N - 1) div (p^λ - 1);
  if I eq 0 then I := v; end if;
  k := GCD(h*I, λ);
  w := λ div k;
  K := GF(p^λ);
  ζ := K ! (N`prim^I);
  M := nearField(p^k, w, K, ζ : LargeMatrices := N`sz eq p);
  f := map< M -> N | x :-> Element(N, (g(x`elt))) >;
  return M, f;
end intrinsic;

intrinsic SubConstr(N :: NfdDck, x :: Any) -> NfdDck, Map
{The sub-nearfield of the Dickson nearfield N generated by x}
  if (Type(x) ne NfdElt) or (x`parent ne N) then
    return "the element must belong to the nearfield", _;
  end if;
  return SubConstr(N, [x]);
```

**end intrinsic**;

# 6 Nearfield planes

The first part of this section is based on the book by Dembowski [14, p. 119*ff*] and a paper of André [2].

A *collineation* of a projective plane $\mathcal{P}$ is an incidence preserving automorphism mapping points to points and lines to lines. A *centre* of a collineation $\alpha$ is a point $c$ such that $\alpha$ fixes every line incident with $c$. An *axis* of $\alpha$ is a line $A$ such that $\alpha$ fixes every point incident with $A$.

A collineation $\alpha$ has a centre if and only if it has an axis. If $\alpha \neq 1$, the centre and axis are unique. If $\alpha$ has a centre (and hence an axis) it is called a *central collineation*.

If $\alpha$ is a central collineation with centre $c$ and axis $A$ we say that $\alpha$ is an *elation* if $c$ is incident with $A$ and that it is an *homology* otherwise.

Let $\Gamma = \mathrm{Aut}(\mathcal{P})$ be the group of all collineations of $\mathcal{P}$. Given a point $c$ and a line $A$, let $\Gamma(c, A)$ be the group of all central collineations with centre $c$ and axis $A$.

If $x$, $y$ and $c$ are three distinct points of $\mathcal{P}$, if neither $x$ nor $y$ lie on the line $A$, and if $x$ and $y$ lie on a line through $c$, there is at most one element $\gamma \in \Gamma(c, A)$ such that $x^\gamma = y$. If for all such $x$ and $y$ there exists $\gamma \in \Gamma(c, A)$ such that $x^\gamma = y$, the group $\Gamma$ is said to be $(c, A)$-*transitive* (Baer [3]). This is equivalent to the transitivity of $\Gamma(c, A)$ on the non-fixed points of any line $\neq A$ through $c$.

The projective plane $\mathcal{P}$ is said to be a *translation plane* with respect to $A$ if $\mathcal{P}$ is $(c, A)$-transitive for every point $c$ on $A$. In this case the group $\Gamma(A, A)$ of all elations with a centre on $A$ is abelian and acts regularly on the points of $\mathcal{P}$ not on $A$.

If $u$ and $v$ are points, then $\mathcal{P}$ is said to be $(u, v)$-*transitive* if it is $(u, L)$-transitive for every line $L$ incident with $v$. In this case $\mathcal{P}$ is a translation plane with respect to $uv$, the line through $u$ and $v$.

A nearfield $N$ is said to be *planar* if the mapping $x \mapsto -xa + xb$ is a permutation of $N$ whenever $a \neq b$. Every finite nearfield is planar.

Given points $u$ and $v$, the projective plane $\mathcal{P}$ is $(u, v)$-transitive if and only if it can be coordinatised by a planar nearfield with the line $uv$ as the line at infinity. This implies that a plane $\mathcal{P}$ is $(u, v)$-transitive if and only if it is $(v, u)$-transitive.

If $\mathcal{P}$ is coordinatised by a nearfield $N$ and $|N| > 9$, then the points $u$ and $v$ are uniquely determined. Thus every collineation of $\mathcal{P}$ fixes the line at infinity and is therefore an affine collineation of $\mathcal{P} \setminus uv$.

## 6.1 Coordinates

Given a finite nearfield $N$, there is an *affine* plane $\mathcal{A}$ with point set $N \times N$ and lines given by the equations

$$y = xm + b$$
$$x = c$$

Let $\mathcal{P}$ be the corresponding projective plane, obtained from $\mathcal{A}$ by adjoining a line $L_\infty$ called the *line at infinity*. We label the points of $\mathcal{P}$ with triples of elements of $N$ as follows.

(1) For every point $(x, y)$ of $\mathcal{A}$ there is a point $[1, x, y]$ of $\mathcal{P}$.

(2) For every $m$ there is an "ideal" point $[0, 1, m]$ of $\mathcal{P}$ which lies on every line $y = xm + b$ $(b \in N)$ and on $L_\infty$.

(3) There is a point $[0, 0, 1]$ of $\mathcal{P}$ which lies on every line $x = c$ and on $L_\infty$.

The lines of $\mathcal{P}$ may also be labelled by triples of elements of $N$: the line $y = xm + b$ corresponds to the triple $[-b, -m, 1]$ and the line $x = c$ corresponds to $[-c, 1, 0]$. The line $L_\infty$ is labelled $[1, 0, 0]$. A point $\pi = [w, x, y]$ is incident with a line $L = [a, b, c]$ if and only if $wa + xb + yc = 0$.

Every collineation of $\mathcal{A}$ extends to a collineation of $\mathcal{P}$.

**Theorem 6.1** (André [2, Satz 9]). *If $\alpha$ is a collineation of the nearfield $N$, which is composed of central collineations, then $\alpha$ is of the form*

$$(x, y) \mapsto (sxa + c, syb + d) \qquad or$$
$$(x, y) \mapsto (syb + d, sxa + c)$$

*where $s \in \mathcal{K}(N)^\times$, $a, b \in N^\times$ and $c, d \in N$.*

To construct a nearfield plane from a nearfield $N$ of order $n$ we begin with the affine plane as described above with lines $y = xm + b$ and $x = c$ and then adjoin the line and points at infinity.

We begin with the set of points $\{P_1, P_2, \ldots, P_t\}$, where $t = n^2 + n + 1$ and represent the lines as subsets of the index set $\{1, 2, \ldots, t\}$.

Multiplication of nearfield elements is quite slow compared to multiplication of the underlying Galois field elements and therefore, to gain speed, we first compute the multiplication table.

```
multiplicationTable := function( N )
   A := AssociativeArray();
   K := N`gf;
   for x in K do for y in K do
         A[<x,y>] := (Element(N,x)*Element(N,y))`elt;
   end for; end for;
   return A;
end function;
```

The points of the nearfield plane are represented as triples of Galois field elements.

```
intrinsic ProjectivePlane( N :: Nfd : Check := false)
        -> PlaneProj, PlanePtSet, PlaneLnSet
{The finite projective plane coordinatised by the nearfield N}
   K := N`gf;
   pts := {@ [K| 1,x,y] : x,y in K @} join
            {@ [K| 0,1,y] : y in K @} join {@ [K| 0,0,1] @};
   lset := {@ @};
   M := multiplicationTable(N);
```

Construct the lines with equations $y = xm + b$.

```
   for m in K do
```

```
    for b in K do
      ln := { Index(pts, [K|1, x, M[<x, m>]+b]) : x in K };
      Include(~ln, Index(pts, [K| 0, 1, m]) );
      Include(~lset, ln);
    end for;
  end for;
```

Include the lines $x = c$, through $[0, 0, 1]$.

```
  for c in K do
    ln := { Index(pts, [K| 1, c, y]) : y in K };
    Include(~ln, Index(pts, [K| 0, 0, 1]) );
    Include(~lset, ln);
  end for;
```

Finally, include the line at infinity.

```
  ln := { Index(pts, [K| 0, 1, y]) : y in K };
  Include(~ln, Index(pts, [K| 0, 0, 1]));
  Include(~lset, ln);
  return FiniteProjectivePlane< #pts | lset : Check := Check>;
end intrinsic;
```

Alternatively we can determine the incidence relation between points and lines by computing the 'inner product' of each point with each line, but this is somewhat slower than the method above.

```
intrinsic ProjectivePlaneAlt( N :: Nfd : Check := false)
        -> PlaneProj, PlanePtSet, PlaneLnSet
{The finite projective plane coordinatised by the nearfield N}
  K := N`gf;
  pts := [ [K| 1, x, y] : x, y in K ] cat [[K| 0, 1, y] : y in K ] cat [ [K| 0, 0, 1] ];
  linelist := [ [K| b, a, 1] : a, b in K ] cat [ [K| b, 1, 0] : b in K ] cat [ [K| 1, 0, 0] ];
  v := #pts;
  M := multiplicationTable(N);
  lineset := {@ {i : i in [1..v] |
    M[<pts[i][1], L[1]>]+M[<pts[i][2], L[2]>]+M[<pts[i][3], L[3]>] eq K ! 0 } :
      L in linelist @};
  return FiniteProjectivePlane< v | lineset : Check := Check>;
end intrinsic;
```

For comparison, here is a version which uses arithmetic within the nearfield.

```
intrinsic ProjectivePlaneOld( N :: Nfd : Check := false)
        -> PlaneProj, PlanePtSet, PlaneLnSet
{The finite projective plane coordinatised by the nearfield N}
  pts := [ [N| 1, x, y] : x, y in N`gf ] cat [ [N| 0, 1, y] : y in N`gf ] cat [ [N| 0, 0, 1] ];
  linelist := [ [N| b, a, 1] : a, b in N`gf ] cat [ [N| b, 1, 0] : b in N`gf ] cat [ [N| 1, 0, 0] ];
  v := #pts;
  lineset := {@ {i : i in [1..v] |
    IsZero(pts[i][1]*L[1]+pts[i][2]*L[2]+pts[i][3]*L[3]) } : L in linelist @};
  return FiniteProjectivePlane< v | lineset : Check := Check>;
```

```
end intrinsic;
```

A slightly faster approach is to construct the plane using an adjacency matrix but this is still significantly slower than the method which uses the projective completion of the affine plane.

```
intrinsic ProjectivePlaneAdj( N :: Nfd : Check := false)
        → PlaneProj, PlanePtSet, PlaneLnSet
{The finite projective plane coordinatised by the nearfield N}
  K := N`gf;
  pts := [ [K| 1,x,y] : x,y in K ] cat [[K| 0,1,y] : y in K ] cat [ [K| 0,0,1] ];
  linelist := [ [K| b,a,1] : a,b in K ] cat [ [K| b,1,0] : b in K ] cat [ [K| 1,0,0] ];
  v := #pts;
  M := multiplicationTable(N);
  A := Matrix(Integers(), v, v,
    [IsZero(M[<pt[1],ln[1]>]+M[<pt[2],ln[2]>]+M[<pt[3],ln[3]>])
          select 1 else 0 : pt in pts, ln in linelist ]);
  return FiniteProjectivePlane< v | A : Check := Check>;
end intrinsic;
```

## 6.2 Hughes planes

In 1957 Hughes [31] discovered a class of finite projective planes constructed from the Dickson nearfields which have rank 2 over their kernel. Neither these planes nor their duals are translation planes and therefore they cannot be obtained by the coordinatisation method of the previous section. Hughes' methods required the kernel to be central but in 1960 the construction was generalised by Rosati [56] to include the Zassenhaus nearfields (see also Dembowski [14, §5.4] and [15]). For simplicity of notation we shall use the term 'Hughes plane' to include both Hughes planes and generalised Hughes planes.

Given a nearfield $N$ of order $q^2$ and whose kernel is $\mathrm{GF}(q)$, the points of the Hughes plane $\mathcal{H}$ are equivalence classes of triples of elements of $N$ where $[x, y, z] \sim [xk, yk, zk]$ for all $k \in N$, $k \neq 0$. For each equivalence class we choose as representative the unique triple whose leading non-zero entry is 1. Let $\mathcal{P}$ be the set of representatives of the points.

The group $\Gamma = \mathrm{GL}(3, q)$ acts on the equivalence classes of points. If $A = (a_{ij})$ is a $3 \times 3$ non-singular matrix, then the transformation

$$[x_1, x_2, x_3] \mapsto [\sum_{i=1}^{3} a_{1i}x_i, \sum_{i=1}^{3} a_{2i}x_i, \sum_{i=1}^{3} a_{3i}x_i]$$

maps points to points.

Given $f \in N$, define the *line* $L(f)$ to be the set

$$L(f) = \{\, [x, y, z] \in \mathcal{P} \mid x + y + fz = 0 \,\}.$$

The lines of the Hughes plane of $N$ are the images of the lines $L(f)$ under the action of the group $\Gamma$.

It was shown by Rosati [55] in the case of Dickson nearfields and by Dembowski [15] in general, that $\Gamma$ has two orbits, $\mathfrak{p}$ and $\mathfrak{q}$, on points. The orbit $\mathfrak{p}$ is the set of points with

representatives $[x, y, z]$, where $x$, $y$ and $z$ belong to $\mathcal{K}(N)$. By a general result of Brauer on symmetric block designs it follows that $\Gamma$ has two orbits on lines.

The points $\mathfrak{p}$ together with the lines joining them are the points and lines of the Desarguesian plane of order $q$; it is a Baer subplane of the Hughes plane. The automorphism group of $\mathcal{H}$ is the semidirect product of $\mathrm{PGL}(3, q)$ by $\mathrm{Aut}(N)$.

TODO: Check this

```
intrinsic HughesPlane( N :: NFD : Check := false)
        → PlaneProj, PlanePtSet, PlaneLnSet
{ The Hughes plane based on the nearfield N }
  if Type(N) eq NFDDck then
    require N`v eq 2 :
       "the nearfield must have rank 2 over its kernel";
  end if;
  K := N`gf;
  points := {@ [K| 1, x, y] : x, y in K @} join
          {@ [K| 0, 1, y] : y in K @} join {@ [K| 0, 0, 1] @};
  M := multiplicationTable(N);
```

A triple is *normalised* if its leading non-zero coefficient is 1.

```
  normalise := function(v)
    if not IsZero(v[1]) then
      a := Element(N, v[1])^-1;
      b := a`elt;
      return [K| 1, M[<v[2], b>], M[<v[3], b>]];
    end if;
    if not IsZero(v[2]) then
      a := Element(N, v[2])^-1;
      return [K| 0, 1, M[<v[3], a`elt>]];
    end if;
    return [K|0, 0, 1];
  end function;
```

Given a triple $v$ of elements of $N$ and a matrix $A \in \mathrm{GL}(3, q)$, apply $A$ to $v$ to get $(Av^{\mathrm{tr}})^{\mathrm{tr}}$ (which is not necessarily the same as $vA^{\mathrm{tr}}$).

```
  apply := func< v, A |
    [ &+[ M[<A[i,j], v[j]>] : j in [1..#v]] : i in [1..#v]] >;
```

The initial set of lines are the solutions of equations $x+y+fz = 0$, where $f = 0$ or $f = \zeta$.

```
  lines := {@ @};
  ln := { [K| 1, -1, z] : z in K };
  Include(~ln, [K| 0, 0, 1] );
  line := { Index(points, v) : v in ln };
  Include(~lines, line);
  f := N`prim;
  ln := { [K| 1, -1-M[<f, z>], z] : z in K };
  Include(~ln, normalise([K| 0, f, -1]) );
  line := { Index(points, v) : v in ln };
  Include(~lines, line);
```

The complete set of lines is the union of the orbits of $\mathrm{GL}(3,q)$ on the lines already obtained.

```
  n := #points;
  S := Sym(n);
  gens := [S|];
  for g in Generators(GL(3,N`q)) do
    perm := [];
    for i := 1 to n do
      v := normalise(apply(points[i],g));
      Append(~perm,Index(points,v));
    end for;
    Append(~gens,S ! perm);
  end for;

  H := sub< S | gens >;
  L := &join[ ln^H : ln in lines ];
  return FiniteProjectivePlane< n | L : Check := Check >;
end intrinsic;
```

# References


[1] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. *SONATA – system of near-rings and their applications, GAP package, Version 2*, 2003. (`http://www.algebra.uni-linz.ac.at/Sonata/`).

[2] Johannes André. Projektive Ebenen über Fastkörpern. *Math. Z.*, 62:137–160, 1955.

[3] Reinhold Baer. Homogeneity of projective planes. *Amer. J. Math.*, 64:137–152, 1942.

[4] Helmut Bender. Endliche Fastkörper und Zassenhausgruppen. In *Group theory, algebra, and number theory (Saarbrücken, 1993)*, pages 97–143. de Gruyter, Berlin, 1996.

[5] Gerhard Betsch, editor. *Near-rings and near-fields*, volume 137 of *North-Holland Mathematics Studies*, Amsterdam, 1987. North-Holland Publishing Co.

[6] Albrecht Beutelspacher. Projective planes. In *Handbook of incidence geometry*, pages 107–136. North-Holland, Amsterdam, 1995.

[7] F. Buekenhout, editor. *Handbook of incidence geometry*. North-Holland, Amsterdam, 1995. Buildings and foundations.

[8] Robert D. Carmichael. *Introduction to the theory of groups of finite order*. Dover Publications Inc., New York, 1956.

[9] James R. Clay. *Nearrings*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1992. Geneses and applications.

[10] Celestina Cotti Ferrero and Giovanni Ferrero. *Nearrings*, volume 4 of *Advances in Mathematics (Dordrecht)*. Kluwer Academic Publishers, Dordrecht, 2002. Some developments linked to semigroups and groups.

[11] Susan Dancs. The sub-near-field structure of finite near-fields. *Bull. Austral. Math. Soc.*, 5:275–280, 1971.

[12] Susan Dancs. On finite Dickson near-fields. *Abh. Math. Sem. Univ. Hamburg*, 37:254–257, 1972.

[13] Peter Dembowski. Scharf transitive und scharf fahnentransitive Kollineationsgruppen. *Math. Ann.*, 149:217–225, 1962/1963.

[14] Peter Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[15] Peter Dembowski. Generalized Hughes planes. *Canad. J. Math.*, 23:481–494, 1971.

[16] Peter Dembowski. Gruppenerhaltende quadratische Erweiterungen endlicher desarguesscher projektiver Ebenen. *Arch. Math. (Basel)*, 22:214–220, 1971.

[17] Leonard Eugene Dickson. Definitions of a field by independent postulates. *Trans. Amer. Math. Soc.*, 4(1):13–20, 1903.

[18] Leonard Eugene Dickson. Definitions of a group and a field by independent postulates. *Trans. Amer. Math. Soc.*, 6(2):198–204, 1905.

[19] Leonard Eugene Dickson. Errata: Definitions of a group and a field by independent postulates. *Trans. Amer. Math. Soc.*, 6(4):547, 1905.

[20] Leonard Eugene Dickson. On finite algebras. *Nachr. Kgl. Ges. Wiss. Göttingen, Math.-phy. Klasse*, pages 358–393, 1905.

[21] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[22] Erich Ellers and Helmut Karzel. Kennzeichnung elliptischer Gruppenräume. *Abh. Math. Sem. Univ. Hamburg*, 26:55–77, 1963.

[23] Erich Ellers and Helmut Karzel. Endliche Inzidenzgruppen. *Abh. Math. Sem. Univ. Hamburg*, 27:250–264, 1964.

[24] David A. Foulser. A generalization of André's systems. *Math. Z.*, 100:380–395, 1967.

[25] David Arthur Foulser. *On finite affine planes and their collineation groups*. PhD thesis, University of Michigan, 1963.

[26] Hugh Francis Gingerich. *Generalized Fields and Desargues Configurations*. Abstract of a Thesis, University of Illinois, 1945.

[27] Susan Dancs Groves. *Locally finite near-fields*. PhD thesis, Australian National University, 1974.

[28] Susan Dancs Groves. Locally finite near-fields. *Abh. Math. Sem. Univ. Hamburg*, 48:89–107, 1979.

[29] Marshall Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[30] Marshall Hall, Jr. *Combinatorial theory*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Inc., New York, second edition, 1986. A Wiley-Interscience Publication.

[31] D. R. Hughes. A class of non-Desarguesian projective planes. *Canad. J. Math.*, 9:378–388, 1957.

[32] Daniel R. Hughes and Fred C. Piper. *Projective planes*. Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[33] Noboru Itô. *Frobenius and Zassenhaus groups*. University of Chicago, Chicago Circle, 1968/69. Lecture Notes (two volumes).

[34] Michael Kallaher. Translation planes. In *Handbook of incidence geometry*, pages 137–192. North-Holland, Amsterdam, 1995.

[35] Helmut Karzel. Unendliche Dicksonsche Fastkörper. *Arch. Math. (Basel)*, 16:247–256, 1965.

[36] Hubert Kiechle, Alexander Kreuzer, and Momme Johs Thomsen, editors. *Nearrings and nearfields*, Dordrecht, 2005. Springer.

[37] C. W. H. Lam, G. Kolesova, and L. Thiel. A computer search for finite projective planes of order 9. *Discrete Math.*, 92(1-3):187–195, 1991.

[38] Heinz Lüneburg. *Lectures on projective planes*. University of Illinois, Chicago, 1969.

[39] Heinz Lüneburg. Über die Anzahl der Dickson'schen Fastkörper gegebener Ordnung. In *Atti del Convegno di Geometria Combinatoria e sue Applicazioni (Univ. Perugia, Perugia, 1970)*, pages 319–322. Ist. Mat., Univ. Perugia, Perugia, 1971.

[40] Heinz Lüneburg. Characterizations of the generalized Hughes planes. *Canad. J. Math.*, 28(2):376–402, 1976.

[41] Heinz Lüneburg. *Translation planes*. Springer-Verlag, Berlin, 1980.

[42] Peter Mayr. Fixed-point-free representations over fields of prime characteristic. Reports of the Mathematical Institutes 554, Johannes Kepler University Linz, 2000.

[43] U. Meierfrankenfeld. Perfect Frobenius complements. *Arch. Math. (Basel)*, 79(1):19–26, 2002.

[44] J. D. P. Meldrum. *Near-rings and their links with groups*, volume 134 of *Research Notes in Mathematics*. Pitman (Advanced Publishing Program), Boston, MA, 1985.

[45] M. L. Narayana Rao, D. J. Rodabaugh, F. W. Wilke, and J. L. Zemmer. A new class of finite translation planes obtained from the exceptional near-fields. *J. Combinatorial Theory Ser. A*, 11:72–92, 1971.

[46] T. G. Ostrom. Vector spaces and construction of finite projective planes. *Arch. Math. (Basel)*, 19:1–25, 1968.

[47] T. G. Ostrom. *Finite translation planes*. Lecture Notes in Mathematics, Vol. 158. Springer-Verlag, Berlin, 1970.

[48] Donald Passman. *Permutation groups*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[49] Martin R. Pettet. Near-fields and linear transformations of finite fields. *Linear Algebra Appl.*, 48:443–456, 1982.

[50] Günter Pilz. *Near-rings*, volume 23 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, second edition, 1983. The theory and its applications.

[51] Fritz Pokropp. Dicksonsche Fastkörper. *Abh. Math. Sem. Univ. Hamburg*, 30:188–219, 1967.

[52] T. G. Room. Geometry in a class of near-field planes. I. General planes of the class. *J. London Math. Soc. (2)*, 1:591–605, 1969.

[53] T. G. Room. The combinatorial structure of the Hughes-Zassenhaus plane of order 25. *Proc. Cambridge Philos. Soc.*, 74:237–245, 1973.

[54] T. G. Room and P. B. Kirkpatrick. *Miniquaternion geometry. An introduction to the study of projective planes*. Cambridge University Press, London, 1971. Cambridge Tracts in Mathematics and Mathematical Physics, No. 60.

[55] Luigi Antonio Rosati. I gruppi di collineazioni dei piani di Hughes. *Boll. Un. Mat. Ital. (3)*, 13:505–513, 1958.

[56] Luigi Antonio Rosati. Su una generalizzazione dei piani di Hughes. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 29:303–308 (1961), 1960.

[57] Luigi Antonio Rosati. Unicità e autodualità dei piani di Hughes. *Rend. Sem. Mat. Univ. Padova*, 30:316–327, 1960.

[58] Luigi Antonio Rosati. Disegni unitari nei piani di Hughes. *Geom. Dedicata*, 27(3):295–299, 1988.

[59] Harald Unkelbach. Eine Charakterisierung der endlichen Hughes-Ebenen. *Geometriae Dedicata*, 1(2):148–159, 1973.

[60] Heinz Wähling. Invariante und vertauschbare Teilfastkörper. *Abh. Math. Sem. Univ. Hamburg*, 33:197–202, 1969.

[61] Heinz Wähling. *Theorie der Fastkörper*, volume 1 of *Thales Monographs*. Thales-Verlag, Essen, 1987.

[62] Joseph A. Wolf. *Spaces of constant curvature*. Publish or Perish Inc., Houston, TX, fifth edition, 1984.

[63] Jill Yaqub. Planes with given groups. In *Foundations of geometry (Proc. Conf., Univ. Toronto, Toronto, Ont., 1974)*, pages 277–336. Univ. Toronto Press, Toronto, Ont., 1976.

[64] Jill Yaqub. Revision of "Finite geometries" by P. Dembowski. Corrections plus an additional chapter, March 1981.

[65] Guido Zappa. Sui gruppi di collineazioni dei piani di Hughes. *Boll. Un. Mat. Ital. (3)*, 12:507–516, 1957.

[66] Hans Zassenhaus. Kennzeichnimg endlicher linearer gruppen als permutationsgruppen. *Abh. Math. Sem. Univ. Hamburg*, 11:17–40, 1935.

[67] Hans Zassenhaus. Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg*, 11:187–220, 1935.