Chapter 8

Semifields.

Recall that a distributive quasifield is called a *semifield.* Equivalently, a semifield is a 'non-associative [skew]field' as seen in the following characterization. The aim of this chapter is to address the following question: what are the possible sizes of finite *non-associative* semifelds? We shall see that semifields that are of order p^2 are always fields. Also all translation planes of order 8 are known to be Desarguesian. But the twisted fields of A. A. Albert and the even order commutative semifelds of D. E. Knuth, taken together, demonstrate that *for all other prime-powers orders* n at least one non-associative semifield plane of order n exists. The main goal of this chapter is to introduce these planes and demonstrate that they are non-associative. This is preceeded by some after some basic results have been established.

8.1 General Remarks On Semifelds.

The following theorem is an analogue of the elementary result: finite [associative] integral domains are fields. Here we prove that finite 'non-associative' integral domains are semifields. Many important constructions of finite [pre]semifelds are based on this principle.

Remark 8.1.1 *A system* $(D, +, \circ)$ *is a semifield iff the following axioms hold:*

1. $(D, +)$ *is an abelian group;*

2. *The distributive laws are valid for* $x, y, z \in D$*:*

(a) $x \circ (y + z) = x \circ y + x \circ z$;

(b) $(y + z) \circ x = y \circ x + z \circ x$.

3. $(D^*, \circ)$ *is a loop.*

A semifield that is not a [skew]field is called a proper semifield. We shall be concerned with *finite* semifields from now on. Thus the basic question is what are the possible orders of proper non-associative semifields? This question has a complete answer, but first we draw attention to some elementary facts.

Remark 8.1.2 *Let $(D, +, \circ)$ be a finite semifield. Then its three seminuclei $N\ell$, N_m and N_r are all fields, in particular its kern coincides with N_ℓ and $(D, +)$ is a vector space over each of these nuclei, as well as over its nucleus and center (both of which are also fields).*

Proof: Exercise. ■

Remark 8.1.3 *A semifield two dimensional over a field in its center is a field. Hence all semifields of order p^2 are known.*

Proof: Exercise. ■
Thus all semifield planes of order p^2 are known. A spectacular extension of this result follows form a theorem of Menichetti: all semifield planes of order p^3 are known. They are forced to be coordinatized by the generalized twisted fields of Albert, see 147.

8.2 The Knuth Commutative Semifields.

Finite commutative semifields (that are not associative) appear to be quite hard to find. The following construction due to Knuth, [30], established the existence of commutative semifields of *even* order N, where $N > 8$ is not a power of 2.

Theorem 8.2.1 (The Binary Knuth Semifields.) *Let $K = GF(2^{nm}) \supset GF(2^m) = K_0$, where $n > 1$ is odd. Let $f : K \to K_0$ be any nonzero linear functional of K as a K_0 vector space. Define a new multiplication as follows:*

$$a \circ b = ab + (f(a)b + f(b)a)^2.$$

The algebraic system $(K, +, \circ)$ is a pre-semifield.

Proof: The fact that $x \mapsto x^2$ is additive in the characteristic 2 case, yields the distributive laws. So it remains to verify $a \circ b = 0$ is impossible if a and b are non-zero. Denying this, we have non-zero a and b such that

$$ab + (f(a)^2 b^2 + f(b)^2 a^2) = 0,$$

so

$$\frac{a}{b} + f(a)^2 + f(b)^2 \left(\frac{a}{b}\right)^2 = 0,$$

which may be written as a quadratic in $x = a/b$:

$$f(b)^2 x^2 + x + f(a)^2 = 0,$$

and this quadratic in x, with coefficients in K_0, is reducible in K because $x = a/b$ is a solution. But since K is odd dimension over K_0, the quadratic must be reducible even in K_0, so $x = a/b \in K_0$. Hence by the definition of $\circ$:

$$\begin{aligned} a \circ b &= ab + (f(a)b + f(b)a)^2 \\ &= ab + (f(bx)b + f(b)a)^2 \\ &= ab + (f(b)bx + f(b)bx)^2, \text{ by linearity of f} \\ &= ab, \text{ in charactersitic 2.} \end{aligned}$$

so $a \circ b = ab \neq 0$, a contradiction. ∎

Exercise 8.2.2 *Show how to obtain a commutative semifeld of the same order as the above pre-semifield.*

The usual procedure for converting a pre-quasifield to a quasifield '$(a \circ b) = (a \circ e) * (e \circ b)$', where e is an arbitrary non-zero element, of course solves exercise 8.2.2 above. However, to ensure that the resulting comutative semifield is not a field f needs to be chosen with some care. Such an f is introduced in the following theorem.

The theorem also demonstrates that in converting a presemifield to a semifield it is desirable to choose the identity 'e' with care, to avoid creating a semifield with a more opaque structure than the presemifield used to construct it.

Theorem 8.2.3 (The Binary Knuth Semifields.) *Let $K = GF(2^{nm}) \supset GF(2^m) = K_0$, where $n > 3$ is odd. Fix a K_0-basis of K of type $(1, \alpha, \alpha^2, \ldots \alpha^{n-1}$ and choose the K_0-valued functional $f : K \to K_0$ such that $f(\alpha^i) = 0$ for $0 \leq i \leq n-2$, and $f(\alpha^{n-1}) = 1$. Define new multiplications $\circ$ and $\odot$ on K as follows for all $a, b \in K$:*

$$\begin{aligned} a \circ b &= ab + (f(a)b + f(b)a)^2 \\ a \circ b &= (a \circ 1) \odot (1 \circ b) \end{aligned}$$

The algebraic system $(K, +, \circ)$ is a commutative presemifield and $(K, +, \odot)$ is a commutative semifield (but not a field) such that they both coordinatize the same semifield plane.

Proof: In view of theorem 8.2.1, it follows easily that $(K, +, \odot)$ is a commutative semifield, with identity $1 \circ 1$, and that the two systems coordinatize the same plane. It remains to check that $\odot$ is not associative. The main step is to obtain a direct representation of $\odot$, viz.:

$$a \odot b = (a \circ 1) \circ (1 \circ b) \tag{8.1}$$

Since K_0 is in the null space of f, and also its image, we obtain $1 \circ a = a + f(a)^2$, $f(a)^2 \in K_0$, and hence $f(1 \circ a) = f(a)$. Thus we have

$$1 \circ (1 \circ a) = a + f(a)^2 + (f(a) + 0)^2,$$

yielding the identity in $a \in K$:

$$1 \circ (1 \circ a) = a. \tag{8.2}$$

Now replacing a and b resp. by $1 \circ a$ and $1 \circ b$ in the defining identity for $\odot$ we have:

$$\begin{aligned} (a \circ 1) \circ (1 \circ b) &= ((a \circ 1) \circ 1) \odot (1 \circ (1 \circ b)) \\ &= a \odot b \text{by (8.2)}, \end{aligned}$$

thus (8.1) has been established.
We can now verify that $\odot$ is not associative by demonstrating that a multiplication involving α^k, $k = n - 1/2$, fails to be associative; exponents here and throughout the proof are assumed relative to *field* multplication. Note that

$k = n - 1/2$, and $n > 3$ means that $k < n - 2$, so, by definition, $f(\alpha^k) = 0$. Hence the formula for $\odot$ given in (8.1) above yields

$$\alpha^k \odot \alpha^k = (\alpha^k \circ 1) \circ (\alpha^k \circ 1) = \alpha^k \circ \alpha^k = \alpha^{n-1},$$

since $z \circ z = z^2$ in characteristic 2. Similarly,

$$\alpha^k \odot \alpha = (\alpha^k \circ 1) \circ (\alpha \circ 1) = \alpha^{k+1},$$

as by definition α^k, α and 1 are all in the kernel of f. We now show that $\odot$ is not associative, by deducing a cntradiction from the following power associativity identity:

$$\alpha \odot (\alpha^k \odot \alpha^k) = (\alpha \odot \alpha^k) \odot \alpha^k, \tag{8.3}$$

which implies that

$$\alpha \odot \alpha^{n-1} = \alpha^{k+1} \odot \alpha^k.$$

But remembering that $f(\alpha^{n-1} = 1$, the LHS becomes

$$(\alpha \circ 1) \circ (\alpha^{n-1} \circ 1) = \alpha \circ (\alpha^{n-1} + 1) = \alpha \circ \alpha^{n-1} + \alpha = \alpha^n + (0 + \alpha 1)^2 + \alpha = \alpha^n + \alpha^2 + \alpha,$$

and the RHS becomes

$$\alpha^{k+1} \odot \alpha^k = (\alpha^{k+1} \circ 1) \circ (1 \circ \alpha^k) = \alpha^{k+1} \circ \alpha^k = \alpha^n + (0^2) = \alpha^n,$$

so the associativity fails unless $\alpha^n + \alpha^2 + \alpha = \alpha^n$ and this means $\alpha = 1$ or $\alpha = 0$, contradicting: $\alpha \in K - K_0$. Thus the power associativity claimed in (8.3) fails and the desired result follows. ■

Exercise 8.2.4 *Show that the theorem is valid even for $n = 3$ provided $K_0 = GF(2^m)$, and $m > 1$.*

Perhaps the most important feature of the theorem above is that it ensures the existence of non-Desarguesian projective planes of order 2^p, p any *prime* > 3.

8.3 Twisted Fields.

Let $c \in K = GF(q^n)$ such that $c \notin K^{q-1}$. Then $GF(q)$-linear maps of $K = GF(q^n)$ defined by:

$$\begin{aligned} P^{-1} &: K \to K \\ &\quad x \mapsto x - cx^q \end{aligned} \tag{8.4}$$

$$\begin{aligned} Q^{-1} &: K \to K \\ &\quad x \mapsto x^q - cx \end{aligned} \tag{8.5}$$

are bijective (thus justifying the inverse notation) because $x = xc^q$ or $x^q = cx$ both contradict the assumption $c \notin K^{q-1}$.

Since P^{-1} and Q^{-1} both map 1 to $1 - c = f$, we also have

$$P(f) = Q(f) = 1, \tag{8.6}$$

We now define the semifield associated with (P, Q); the above equation will establish the multiplicative identity.

Theorem 8.3.1 *Define $\odot$ by:*

$$x \odot y = xP(yQ)^q - (xP)^q(yQ)c,$$

and let $f = 1 - c$. Then $(K, +, \odot)$ is a division algebra with identity $f = 1 - c$ and center $F \odot f$ where $F = GF(q) \subset GF(q^n)$.

Proof: Since P and Q are inverses of F-linear bijections they too must be F-linear bijections. Now since P, Q and the field automorphism $x \mapsto x^q$ are all additive, the distributive laws hold. Zero divisors exist only if for some non-zero x and y:

$$xP(yQ)^q = (xP)^q(yQ)c \Longrightarrow (xP/yQ)/(xP/yQ)^q = c,$$

contradicting the hypothesis that c is not a $q-1$-th power. Hence the system is a presemifield.

To verify that f is the multiplicative identity, apply eq (8.6) to

$$x \odot f = xP - (xP)^q c = (xP)P^{-1} = x$$

and similarly:

$$f \odot x = xQ^q - xQc = (xQ)Q^{-1} = x.$$

Thus f is the multiplicative identity. Now we establish that $F \odot f$ may be identified with F, by remembering that S, P and Q are all members of $GL(K,+)$ that *are linear over* F, and that $fP = fQ = 1$; for all $x \in K$ and $\alpha \in F$:

$$\begin{aligned} x \odot (f\alpha) &= xP(f\alpha)Q^q - (xP)^q(f\alpha)Qc \\ &= (xP(f)Q^q - (xP)^q(f)Qc)\,\alpha \\ &= (xP - (xP)^q c)\,\alpha \\ &= (xP)P^{-1}\alpha = x\alpha \end{aligned}$$

and similarly

$$(f\alpha) \odot x = (xQ^q - xQc)\alpha = (xQ)Q^{-1}\alpha = x\alpha.$$

Thus we have shown:

$$(f\alpha) \odot x = x\alpha = x \odot (f\alpha) \forall x \in K \alpha \in F. \tag{8.7}$$

Now it is straightforward to check that $F \odot f$ is in the middle and left nuclei; for example $(x \odot f\alpha) \odot y$ and also $x \odot (f\alpha \odot y)$ may be written, by eq 8.7, as $(x\alpha) \odot y$ and $x \odot (\alpha y)$ respectively and these are equal because all the three maps defining $\odot$ are linear over $\alpha \in F$. The result follows. ∎

It appears to be surprisingly hard to determine whether or not $F \odot f$ is the *full* center of the semifield. In fact, it appears hard to verify even that the semifield is not a field. To verify this we shall determine when the semifield is non-commutative. This requires an explicit form for the Vaughan polynomial for P: our definition of P is specified *indirectly*, in terms of the Vaughan Polynomial of P^{-1}.

As indicated by Albert, the product $\odot$ cannot be regarded as explicitly known until the Vaughan polynomials for P *and* Q are explicitly known. However, in view fo the close connection between the definitions of P^{-1} and Q^{-1}, cf (8.4) and (8.5), it is possible to deduce the Vaughan polynomial of Q from that of P, so we only compute P explicitly.

8.3.1 Polynomial for P; Non-Commutivity of Semifield.

In this section we adopt the following:

Notation 8.3.2 *Regarding $K = GF(q^n) \supset F = GF(q)$ as a rank n vector space over F, and define the F-linear maps of K:*

1. $S : x \mapsto x^q$;

2. $R_a : x \mapsto xa$, *for* $a \in K$;

We regard members of $Hom_F(K,+)$ as acting on K from the right. The associative ring $\sum_{i=0}^{n-1} S^i R_{a_i}$, for $a_i \in K$, forms an F-algebra; F may be identified with the central field $\{R_f \mid f \in F\}$. By Vaughan polynomials the S^i's in the expression are linearly independent over F and hence the expressions account for $|K|^n$ K-linear maps in $Hom_F(K,+)$, but since this set has size $|F|^{n^2}$, we have a fundamental fact concerning Vaughan polynomials.

Result 8.3.3 (Fundamental Theorem of Vaughan Polynomials.) *The K-algebra $Hom_F(K,+)$ is the K-algebra:*

$$\left\{ \sum_{i=0}^{n-1} S^i R_{a_i} \mid a_i \in F, \forall i \in [0, n-1) \right\}.$$

We now compute P using eq(8.4), which may be written as $P^{-1} = x - xSR_c$, and the elementary ring identity

$$(1-\theta)(1+\theta+\theta^2+\ldots+\theta^{n-1}) = 1-\theta^n,$$

by noticing that $\theta := SR_c$ implies:

$$1-\theta = P^{-1}.$$

Thus we have:

$$P^{-1}\left(1+SR_c+(SR_c)^2+\ldots+(SR_c)^{n-1}\right) = 1-(SR_c)^n \qquad (8.8)$$

and now $(SR_c)^i$ may be expressed in the following notation,

$$(SR_c)^i = S^i R_{c_i}, \qquad (8.9)$$

where $c_i \in F^*$ is uniquely defined by the above requirement. In particular, we need to record:

Remark 8.3.4 *Define $c_i \in F$ in terms of c by:*

$$\forall i \in [1,n] : (SR_c)^i = S^i R_{c_i}. \qquad (8.10)$$

Then

1. *P^{-1} commutes with all terms of type $S^i R_{c_i}$*
2. *$c_n \in GF(q)$. $c_{i+1} = (c_i)Sc$.*
3. *$c_n \in GF(q)^*$, but $c_n \neq 1$.*

Proof: The first part holds because, by definition, $P^{-1} = 1 - (SR_c)$ and terms $S^i R_{c_i}$ are all powers of a single term SR_c. In particular, eq (8.10) means that

$$S^{i+1} R_{c_{i+1}} := (SR_c)^{i+1} = (SR_c)^i SR_c = S^{i+1} R_{(c_i)Sc}.$$

The next case follows from eq (8.10) by putting $i = n$ and noting:

$$c_n = S^n c_n = (SR_c)^n = S^n c(cS)(cS^2)\dots(cS^{n-1}) = \nu(c),$$

where the norm $\nu(c)$ relative to S must lie in its fixed field, so $c \in GF(q)$ Now if $1 = \nu(C) = c^{q^n - 1/q-1}$ then we claim c is a $q-1$-th power. Now writing $c = \omega^{k(q-1)+r}$, ω a primitive element of $GF(q^n)^*$ and $0 \leq r < (q-1)$, implies $\omega^{r(q^n-1)/q-1} = 1$, so $r = 0$. ■

Now the commutivity condition for P^{-1}, the fact that $(SR_c)^n = S^n R_{c_n} = R_{c_n}$, and by the final case above, $1 - R_{c_n} \in GF(q)^*$, means that the identity (8.8) may be restated as follows:

$$P = (1 + SR_{c_1} + S^2 R_{c_2} + \ldots + S^{n-1} R_{c_{n-1}})(1 - R_{c_n})^{-1}. \qquad (8.11)$$

The above identity is the Vaughan polynomial for P. If desired, a similar identity for Q may be obtained, or deduced from the expression for P.

We now use the above Vaughan polynomial for P to determine when the divison algebra $(D, +, \odot)$ is commutative. The definition of $\odot$ means that it is commutative iff:

$$xP(yQ)^q - (xP)^q yQc = yP(xQ)^q - (yP)^q (xQ)c$$

so putting $y \mapsto yQ^{-1}$ shows commutivity is equivalent to the identity:

$$xPy^q - (xP)^q yc = yQ^{-1}P(xQ)^q - (yQ^{-1}P)^q (xQ)c$$

and viewing both sides as functions of y, implies that the commutivity is equivalent to:

$$SR_{xP} - R_{(xP)Sc} = Q^{-1}P(R_{xQS} - SR_{(xQ)c}),$$

and using the Vaughan expansion for P in eq (8.11) above, and recalling the definition of Q^{-1}, eq (8.5), we see that commutivity of the semifield is equivalent to the following identity after the $GF(q)^*$ element $(1 - R_{c_n})^{-1}$ is shifted to the LHS.

$$\begin{aligned}(SR_{xP} - R_{(xP)Sc})(1 - R_{c_n}) &= (S - R_c)(1 + SR_{c_1} + S^2R_{c_2} + \dots S^iR_{c_i} \dots \\ &\quad \dots S^{n-1}R_{c_{n-1}})(R_{xQS} - SR_{(xQ)c}),\end{aligned}$$

and on making the substitution $xQ \leftarrow t$ we have:

$$\begin{aligned}(SR_{xP} - R_{(xP)Sc})(1 - R_{c_n}) &= (S - R_c)(1 + SR_{c_1} + S^2R_{c_2} + \dots S^iR_{c_i} \dots \\ &\quad \dots S^{n-1}R_{c_{n-1}})(R_{tS} - SR_{tc}),\end{aligned}$$

We now compute the coefficient of the powers of $S^i > S^2$ on the RHS when this is expressed in standard S-polynomial form:

$$\begin{aligned}((S + S^2R_{c_1} + S^3R_{c_2} + \dots S^{i+1}R_{c_i} \dots) &- R_c(1 + SR_{c_1} + S^2R_{c_2} + \dots + S^iR_{c_i} \dots \\ &\dots + S^{i+1}R_{c_{i+1}} \dots)) \times (R_{tS} - SR_{tc}) = \\ ((S + S^2R_{c_1} + S^3R_{c_2} + \dots + S^{i+1}R_{c_i}) \dots &- (R_c + SR_{cSRc_1} + S^2R_{cS^2c_2} + \dots + S^iR_{cS^ic_i} \\ &\dots + S^{i+1}R_{cS^{i+1}c_{i+1}} \dots)) \times (R_{tS} - SR_{tc}),\end{aligned}$$

and the terms in S^i above, after expansion, have form

$$\begin{aligned}&= S^iR_{c_{i-1}}R_{tS} - S^iR_{cS^ic_i}R_{tS} - S^{i-1}R_{c_{i-2}}SR_{tc} + S^{i-1}R_{cS^{i-1}c_{i-1}}SR_{tc} \\ &= S^iR_{c_{i-1}(tS)} - S^iR_{cS^ic_i(tS)} - S^iR_{c_{i-2}Stc} + S^iR_{(cS^i)(c_{i-1}S)(tc)} \\ &= S^i[R_{c_{i-1}(tS)} - R_{cS^ic_i(tS)} - R_{c_{i-2}Stc} + R_{(cS^i)(c_{i-1}S)(tc)}],\end{aligned}$$

and this coefficient for $i \in [2, n-1]$ must vanish for all t, which means

$$(c_{i-1} - (cS^i)c_i)t^q + (cS^ic_{i-1}S - c_{i-2}S)tc \equiv 0$$

and this is equivalent, for $i > 1$, to

$$\begin{aligned}c_{i-1} - (cS^i)c_i &= 0 \\ \text{and } cS^ic_{i-1}S - c_{i-2}S &= 0,\end{aligned}$$

and the case $i = 2$, remembering $c_1 := c$, yields: $c_1 = cS^2c_2$, but now by $c_2 = cSc$ we have $c^{-1} = cS$, hence also $c_2 = 1$. Now lemma 8.3.4(2), page 144, above shows that the c_i for $i \geq 1$ alternates:

$$c_1 = c, c_2 = 1, c_3 = c, c_4 = 1, c_5 = c, \dots c_n = 1,$$

where $c_n = 1$ is forced because, by lemma 8.3.4 again, c_n is in $GF(q)$, unless c itself is in $GF(q)$. But recall that $1 - c_n \neq 0$ means that only the latter case can occur. But also remember that $c^q = c^{-1}$ means that $c^2 = 1$ as S fixes $GF(q)$ elementwise. So $c = \pm 1$ and $c = 1$ means it is a $q-1$-th power. Hence $c = -1$ is the only possibility, and this actually works: now $P = Q$ is automatic and the above constraints are all met easily.

Thus we have established

Theorem 8.3.5 *Assume $n > 2$. $(D, +, \odot)$ is commutative iff $c = -1 \neq 1$ and $P = Q = (1 + S)$.*

8.4 Generalised Twisted Fields.

The twisted fields of Albert, discussed in the previous section, are important partly because they help to demonstrate that non-associative semifields of odd order p^r exist, for p prime, iff $r > 2$. The generalized twisted fields, introduced in this section, have proven to be of importance because they arise in several major classification theorems: Menichetti's classification of the semifields of order p^3 and in the Cordero-Figueroa-Liebler classification of semifield planes admitting large autotopism groups of various types. In all these cases the associated planes are shown to be among th class of generalized twisted fields of Albert, rather than in the class of planes coordinatized by just the ordinary twisted fields of the previous section.

We begin with an elementary result from arithmetic that has wide applications in the exploitation of finite fields.

Result 8.4.1 *Let q be a prime power. Then*

$$\gcd\left(q^a - 1, q^b - 1\right) = q^{\gcd(a,b)} - 1.$$

Proof: The RHS divides the LHS because, in general, $q^m - 1$ divides $q^n - 1$ if m divides n. Let u be any maximal prime power dividing LHS. Then $q^a \equiv 1 \pmod{u}$ and $q^b \equiv 1 \pmod{u}$ and also q is invertible $\pmod{u}$. So a and b are divisible by the order A of $q \pmod{u}$. So A divides $\gcd(a, b)$, hence u divides $q^{\gcd(a,b)} - 1$, so u divides the RHS. ■

Throughout the section we adopt the following hypothesis:

Notation 8.4.2 *The integer $q = p^s > 1$ is a power of the prime p. $K = GF(q^n)$ and $AutK$ denotes the associated Galois group generated by $\rho : x \mapsto x^q$. Assume $S, T \in AutK$ such that*

1. $1 \neq S \neq T \neq 1$; *and*

2. $Fix(S,T) = GF(q)$.

Note that any finite field with two distinct non-trivial automorphisms, S and T, can be viewed as satisfying all the above conditions if we define $GF(q)$ to be the fixed field of the group $< S, T >$.

Write $N = K^{S-1}K^{T-1}$, so N^* is a multiplicative subgroup of K^*. Fix an element $c \in N - K$.

Exercise 8.4.3 Take $K = GF(q^n)$, $S : x \mapsto x^q$, and $T = S^{-1}$. Show that c can be chosen provided $n > 2$ and $q > 2$. What goes wrong when $n = 2$?

The *Albert product* on K, written $< x, y >_c$ and abbreviated to $x \circ y$ is defined by:

$$\forall x, y \in K : x \circ y :=< x, y >_c := xy - x^T y^S c. \tag{8.12}$$

Remark 8.4.4 $< x, y >_c = 0 \iff x = 0 \vee y = 0$.

Since S and T are additive, $(K, +, \circ)$ must also satisfy both distributive laws: so we have a finite 'non-associative integral domain' and, as in the associative case, this means that multiplication defines a quasigroup on the non-zero elements. Thus we have:

Lemma 8.4.5 *Suppose the triple $(D, +, \circ)$ is such that $(D, +)$ is a FINITE abelian group such that both the distributive laws hold. Then $(D^*, \circ)$ is a quasigroup, or equivalently, $(D, +, \circ)$ is a presemifield if and only if:*

$$x \circ y = 0 \iff x = 0 \vee y = 0.$$

Proof: The distributive laws imply that the maps $x \mapsto x \circ a$ and $x \mapsto b \circ x$ are additive and so the no-zero-divisor hypothesis holds iff both maps are injective and hence bijective. The lemma follows. ∎
In view of eqn 8.12, lemma 8.4.5 above, applied to the Albert product, immediately yields:

Theorem 8.4.6 *Let $\mathcal{A}_c := (K, +, \circ)$, where $\circ =<, >_c$ is an Albert product on $K = GF(q^n)$ and $(K, +)$ is the additive group of of the field. Then $\mathcal{A}_c$ is a pre-semifield.*

The planes coordinatized by the presemifields $\mathcal{A}_c$ will be called the *Albert planes*. The presemifields $\mathcal{A}_c$ will be called *generalized twisted fields*.

The following proposition yields the list of orders that Albert plane have.

Proposition 8.4.7 *Let $K = GF(q^n)$, $Fix(< S,T >) = GF(q)$, where $S \neq T$ are distinct nontrivial $GF(q)$-linear field automorphisms in $AutK$ such that $Fix(< S,T >) = GF(q)$. Let $N = K^{S-1}K^{T-1}$, then $K - N \neq \emptyset$ iff*

1. *$q > 2$ and $n > 2$; now any pair of distinct non-trivial S and T will yield $K - N \neq \emptyset$;*
2. *If $q = 2$ and n is not a prime; now, wlog $1 \leq a < b < n$, the pair*

$$\left(S : x \mapsto x^{p^a}, T : x \mapsto x^{p^b}\right)$$

yields $K - N \neq \emptyset$ iff and $\gcd(a,b) > 1$ shares a non-trivial factor with n.

Proof: We may write $S - 1 = q^s - 1$ and $T - 1 = q^t - 1$. So N^* only contains powers of ω^{q-1} where ω is a primitive generator of $GF(q^n)$. So if $q > 2$ then an Albert sytem exists so long distinct S and T exist such that $Fix(< S,T >) = GF(q)$. This can be arranged by taking $S : x \mapsto x^q$ and T to be a power of S but distinct from it: unless S^2 is the identity, i.e., $n = 2$. If $n = 2$ then obviously no T satisfying are requirements exist.

So it remains to consider the case when $q = 2$, again $n > 2$ is forced. Now putting $S : x \mapsto x^{2^a}$ and $T : x \mapsto x^{2^b}$, we clearly have $1 < a, b < n$, where

$$gcd(a,n) \neq 1 \neq \gcd(b,n)$$

since for integer $x > 1$:

$$N^* \supseteq K^* 2^x - 1 =< \omega^{2^x - 1} >=< \omega >,$$

holds unless $1 \neq \gcd(2^n - 1, 2^x - 1) = \gcd(n,x)$, by result 8.4.1, 147. Thus n cannot be prime, and furthermore a and b must share a proper prime factor with n. Now

$$\begin{aligned} N^* &= < \omega^{2^a-1}\omega^{2^b-1} > \\ &= \left\{\omega^{x(2^a-1)+y\left(2^b-1\right)} \mid x, y \in \mathcal{Z}\right\} \\ &= < \omega^{\gcd\left(2^a-1,2^b-1\right)} > \\ &= < \omega^{\left(2^{\gcd(a,b)}-1\right)} >, \end{aligned}$$

and so $N^* < K^*$ iff

$$K^* \neq < \omega^{\left(2^{\gcd(a,b)}-1\right)} >$$

and this holds iff

$$\left(2^{\gcd(a,b)} - 1, 2^n - 1\right) \neq 1,$$

and this is equivalent to $\gcd(a, b)$ and n sharing a non-trivial factor. ■

Exercise 8.4.8

1. There are no generalized twisted fields of order < 64 and there do exist gtt of order 64.

2. There exists generalized twisted fields of order 2^n, provided n is not a prime *and* $n > 4$.

3. Using Albert's approach for twisted fields, determine when generalized twisted fields coordinatize non-Desarguesian translation planes.

8.5 Some Two-Dimensional Semifields.

In this section we mention two classes of semifields whose planes admit geometric characterizations. They are also associated with tangentially transitive planes. We use the following notation.

Let F be a finite field of odd order and $a \in F^*$ a non-square in F. Let λ be an indeterminate over F, and θ a non-trivial field automorphism of F. Let $D = F \oplus \lambda F$.

Theorem 8.5.1 (Dickson's Commutative Semifields.) *Suppose $a \in F^*$ is non-square, so F is odd. Then*

$$(x + \lambda y) \circ (z + \lambda t = (xz + a(yt)^\theta) + \lambda(yz + xt)$$

is a commutative semifield such that:

1. *F is the middle nucelus of $(D, +, \circ)$;*

2. *$K = Fix(\theta) \cap F$ is the rightnucleus, the left nucelus and hence also the center of D.*

Theorem 8.5.2 (Hughes-Kleinfeld Semifelds.) *Suppose* $a = x^{1+\theta} + xb$ *has no solution for* x *in* F. *Then*

$$(x + \lambda y) \circ (z + \lambda t = (xz + aty^{\theta}) + \lambda(yz + (x^{\theta} + y^{\theta}b)t$$

is a semifield and F *is its right and middle nucleus. Conversely, if* D *is a semifield that is a finite two dimensional over a field* F *such that the middle and right nucelus of* D *coincide then* D *is a Hughes-Kleinfeld semifield.*