Chapter 9

Generalised André Systems and Nearfields.

In this section we introduce important classes of quasifields that do not coordinatize semifeld planes.

9.1 Construction Of Generalised André Systems.

Let F be an extension field of a field K, $\Lambda = Gal(F/K)$, and let $\lambda : F^* \to \Lambda$ be any map such that the $\lambda(1) = 1$. Then $Q_\lambda = (F, +, \circ)$ is defined by taking $(F, +)$ as the additive group of the field F and $\circ$ is defined, in terms of field multiplication, so that for $x, f \in F$:

$$\begin{aligned} x \circ f &= x^{\lambda_f} f \quad f \neq 0 \\ x \circ 0 &= 0. \end{aligned}$$

So Q_λ obeys the right distributive law, has a multiplicative identity, has a unique solution for $\square \circ f = g$, whenever $f \neq 0$, and multiplying by zero yields zero. Hence, in the finite case, Q_λ is a quasifield iff the equation $f \circ \square = g$ has a unique solution for $\square$ when $f, g \in F^*$. For a treatment of the general case, including when K is a skewfield, see Lüneburg [31]. The system Q_λ is called a λ-system, or a generalized André system, *if turns out to be a quasifield*; the corresponding translation plane is called a generalized André plane.

We shall only consider finite generalized André planes here. An effective way to study them is to describe them in number-theoretic terms. We denote the set of the first k natural numbers $0, 1, \ldots, k-1$ by I_k.

Definition 9.1.1 *Let $F = GF(q^d) \supset K = GF(q)$, $n = q^d > q$, and let $\rho : x \mapsto x^q$ be the generator of $Gal(F/K)$. Choose a primitive generator ω of the multiplicative group F^*. Let $\lambda : i \mapsto \lambda_i$ be any map from I_{n-1} into I_d such that $\lambda_0 = 0$. Define $Q_\lambda := (F, +, \circ)$, where $+$ is field addition, and $\circ$ is given by:*

$$\omega^i \circ \omega^j := (\omega^i)^{q^{\lambda_j}} \omega^j = \omega^{iq^{\lambda_j}+j},$$

and $x \circ 0 = 0 = 0 \circ x$ for all $x \in F$. We regard Q_λ as the λ-structure associated with (λ, q, q^d).

We now consider which choices of λ make Q_λ a quasifield. As indicated above, Q_λ will be a quasifield provided the equation $f \circ \square = g$ has, for $f, g \in F^*$, a unique solution for $\square$, and by our finiteness hypothesis, this is equivalent to the the injectivity of all the maps $z \mapsto \phi \circ z$, for $\phi \in F^*$. However, this condition *fails* iff there exists $x, y \in I_n$, $x \not\equiv y \pmod n$, so wlog $\lambda_x \geq \lambda_y$, such that

$$\begin{aligned} & \exists f \in I_n : \omega^f \circ \omega^x = \omega^f \circ \omega^y \\ \iff & \exists f \in I_n : fq^{\lambda_x} + x \equiv fq^{\lambda_y} + y \pmod{n-1} \\ \iff & \exists f \in I_n : x - y \equiv f\left(q^{\lambda_x} - q^{\lambda_y}\right) \pmod{n-1}, \end{aligned}$$

so Q_λ fails to be a quasifield is equivalent, for $\lambda_x \geq \lambda_y$, to the following condition:

$$\iff \exists f \in I_n : x - y \equiv fq^{\lambda_y}\left(q^{\lambda_x - \lambda_y} - 1\right) \pmod{n-1}. \qquad (9.1)$$

But choosing $t = t_{(x,y)} = \gcd(\lambda_x - \lambda_y, d-1)$ in the above condition (9.1) above means that

$$\frac{x-y}{q^t-1} \equiv fq^{\lambda_y}\frac{q^{\lambda_x-\lambda_y}-1}{q^t-1} \pmod{\frac{q^d-1}{q^t-1}},$$

and now, since by an elementary result 8.4.1, page 147, we have

$$\gcd\left(q^{\lambda_y}\frac{q^{\lambda_x-\lambda_y}-1}{q^t-1}, \frac{q^d-1}{q^t-1}\right) = 1,$$

a solution for f in equation (9.1) exists iff $\frac{x-y}{q^t-1}$ is an integer, that is $x \equiv y \pmod{q^t - 1}$. Thus, the condition that $z \mapsto \phi \circ z$ is injective for for all non-zero f, is equivalent to ensuring that $x \equiv y \pmod{q^t - 1}$ cannot hold, unless $x \equiv y \pmod{n}$. Thus we have

Theorem 9.1.2 (Fundamental λ-Law.) *[12, Lemma 2.1] Let Q_λ be a λ-structure on $GF(q^d)$, defined in terms of the field automorphism $\rho : x \mapsto x^q$ of $GF(q^d)$, and the primitive element ω of order $n-1$, $n := q^d$. Assign to every two distinct integers $x, y \in I_n$:*

$$t_{x,y} := \gcd(\lambda_x - \lambda_y, d)$$

Then Q_λ is a quasifield iff:

$$x \equiv y \pmod{q^{t_{x,y}} - 1} \Longrightarrow x \equiv y \pmod{n-1}.$$

In particular, if λ yields a quasifield for some choice of the primitive ω then it works for all choices of ω. However, changing ω, while holding λ fixed, will in general yield non-isomorphic quasifields.

The following exercise will be used in normalising λ-systems.

Exercise 9.1.3 *Suppose*

$$GF(q^d) \supset GF(q^s) \supset GF(q)$$

and let $\rho : x \mapsto x^q$ denote the primitive automorphism in $Gal(q^d/q)$. Then:

(1) s divides d;

(2) If $\rho^k \in Gal(q^d/q^s)$ then s divides k.

Proof: Part (1): the larger field is a vector space over the smaller field. Part (2): By Euclid algoritm $k = sx + y$, $0 \le y < s$, so $\rho^k \in Gal(q^d/q^s)$ implies that ρ^y also lies in the same field, so y is a multiple of s, since the Frobenius automorphism for the field is ρ^s. Hence $y = 0$. ∎

Proposition 9.1.4 *Let $\lambda : I_{q^d-1} \rightarrow I_d$, q a prime-power, define the generalsied André system $Q_\lambda = (F, +, \circ)$ on $F = GF(q^d)$, based on the Frobenius automorphism $\rho : x \mapsto x^{q^d}$ and the primitive element $< \omega >$. Then:*

(1) $\Phi_\lambda := Fix\{\rho^{\lambda_i} \mid i \in I_{q^d-1}\}$, *is a subfield* $GF(q^s)$ *of* F *such that* s *divides* d *and also divides* λ_i, *for all* $i \in I_{q^d-1}$; *and*

(2) The function $\mu : I_{q^d-1} \to I_{\frac{d}{s}}$ *defined by* $\mu : i \mapsto \frac{\lambda_i}{s}$ *yields a* λ*-system* $Q_\mu = (F, +, *)$ *by:*

$$\omega^i * \omega^j = (\omega^i)^{R_j^\mu} \omega^j,$$

relative to ω *and* $R = \rho^S$, *the Frobenius automorphism of* $Gal(q^d/q^S)$.

Moreover, $\Phi_\mu := Fix\{\rho^{\mu_i} \mid i \in I_{q^d-1}\}$, *is the fixed field of the Frobenius automorphism* $R : x \mapsto x^{q^S}$ *defining* Q_μ *and* $(F, +, *) = (F, +, \circ)$.

Proof: In view of the previous exercise, it essentially remains to verify that the two products coincide:

$$\begin{aligned} \omega^i * \omega^j &= (\omega^i)^{R_j^\mu} \omega^j \\ &= (\omega^i)^{(\rho^S)^{(\lambda_j/S)}} \omega^j \\ &= (\omega^i)^{(\rho)^{(\lambda_j)}} \omega^j \\ &= \omega^i \circ \omega^j, \end{aligned}$$

as required. ∎

Hence, any finite generalized André system may be expressed in the form $Q_\lambda = (F, +, \circ)$ where $\circ$ is determined by a λ-function $\lambda : I_{q^d-1} \to I_d$, associated with $GF(q^d)$, such that

$$\Phi_\lambda := Fix\{\rho^{\lambda_i} \mid i \in I_{q^d-1}\} = GF(q),$$

the fixed field of the Frobenius automorphism $\rho : x \mapsto x^q$ used in defining $\circ$ from λ.

Thus without loss of generality we assume that if $\lambda : I_{q^d-1} \to I_d$ defines a generalized Adré sysytem then the λ is chosen so that the fixed field of the group generted by $\left\{\rho^{\lambda_i} \mid: i \in I_{q^d-1}\right\}$ is just $GF(q)$, the fixed field of the Frobenius automorphism $x \mapsto x^d$.

9.2 No Shears In λ-Systems.

Proposition 9.2.1 *In the* λ*-system* Q_λ *suppose* $a, b, a+b \in Q_\lambda^*$ *and that for all* $c \in Q_\lambda$:

$$c \circ (a + b) = c \circ a + c \circ b.$$

Then $\lambda_a = \lambda_b$.

Proof: Solving for $\lambda_{(a+b)}$:

$$c\lambda_{(a+b)} = \frac{(c)\lambda_a a + (c)\lambda_b b}{(a+b)},$$

and writing $c = xy$ we get:

$$(xy)\lambda_{(a+b)} = \frac{(xy)\lambda_a a + (xy)\lambda_b b}{(a+b)},$$

and noting that all λ's are multiplicative bijections:

$$(x)\lambda_{(a+b)}(y)\lambda_{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

and by the formula for $c\lambda(a+b)$:

$$\frac{(x)\lambda_a a + (x)\lambda_b b}{(a+b)} \frac{(y)\lambda_a a + (y)\lambda_b b}{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

yielding:

$$(x)\lambda_{(a+b)}(y)\lambda_{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

and by the formula for $c\lambda_{(a+b)}$:

$$\begin{aligned} ((x)\lambda_a a + (x)\lambda_b b)\,((y)\lambda_a a + (y)\lambda_b b) &= \\ (x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b(a+b), & \\ \text{and expanding yields:} & \\ (x)\lambda_a(y)\lambda_a a^2 + (x)\lambda_b(y)\lambda_b b^2 + (x)\lambda_a(y)\lambda_b ab + (x)\lambda_b(y)\lambda_a ab &= \\ (x)\lambda_a(y)\lambda_a a(a+b) &+ (x)\lambda_b(y)\lambda_b b(a+l \end{aligned}$$

yielding the field automorphism identity in x and y (zero values permitted):

$$(x)\lambda_a(y)\lambda_a + (x)\lambda_b(y)\lambda_b = (x)\lambda_a(y)\lambda_b + (x)\lambda_b(y)\lambda_a$$

and by Vaughan polynomials in two variables these additive identities cannot be equal unless $\lambda_a = \lambda_b$. ∎

Corollary 9.2.2 *A finite generalized André system cannot be a semifield unless λ is identically zero, in which case it is just a field.*

Exercise 9.2.3 *Let $n = q^d$, q a prime power, and suppose $\lambda : I_{n-1} \rightarrow I_d$ be a map such that $\lambda_0 = 0$. Put $t_{xy} = \gcd(\lambda_x - \lambda_y, d)$, for $x, y \in I_n$. Assume λ is a λ-system in the sense that:*

$$x \equiv y \pmod{q^{t_{xy}} - 1} \Longrightarrow x \equiv y \pmod{q^d - 1}.$$

1. *The zero map is a λ-function, and the corresponding quasifield Q_λ is a field.*
2. *Find all the λ-systems when $d = 2$.*
3. *$t_{xy} = 1$ for all distinct $x, y \in I_n$ iff d is prime.*
4. *If d is prime then λ is constant on the additive cosets of the ideal of I_n generated by $q - 1$. Conversely, any function constant on the additive cosets of the principal ideal $I_{n-1}(q-1)$ is a λ function.*
5. *Show that, apart from fields, no quasifields Q_λ of order $n = 2^p$ can exist if p is prime.*
6. *If $i \equiv j \pmod{q^{t_{ij}} - 1}$ for distinct $i, j \in I_{n-1}$ then $\lambda_i = \lambda_j$.*

9.3 Cyclic Groups In λ-Sytems.

Proposition 9.3.1 (Period v_λ of a λ-system.) *Call the integer $k \in I_{n-1}$ a* scale *for a λ function iff:*

$$x \equiv y \pmod{k} \Longrightarrow \lambda_x = \lambda_y.$$

Then the set of scales may be expressed as an ideal $v_\lambda I_{n-1}$ of I_{n-1}, where the integer $v_\lambda | n - 1$. The integer $v := v_\lambda$ is called the **period** *of λ.*

Proof: If k is a scale then ka is a scale because $x \equiv y \pmod{ka}$ implies $x \equiv y \pmod{k}$. If m and k are scales we must show $m - k$, where $m \geq k$ wlog, is also a scale. Suppose $|x - y| = m - k$, and wlog $x = y + m - k$. Now $\lambda_y = \lambda_{y+m}$ because m is a scale, and $\lambda_{y+m} = \lambda_x$ because k is a scale. So $\lambda_x = \lambda_y$. Thus the scales form an additive subgroup of I_{n-1} and the rest follows because the integers form a principal ideal domain with I_{n-1} as an image. ∎

The $v_\lambda := v$ shows that Q_λ has a cyclic subgroup.

Corollary 9.3.2 *$< \omega^{v_\lambda} >$ is a cyclic subgroup of Q_λ with the same multiplication when the field multiplication on $< \omega >$ is restricted to $< \omega^{v_\lambda} >$.*

Proof: By scaling law:

$$\lambda_{va} = \lambda_v = \lambda_0 = 0.$$

■

The following implies a lower bound for the cyclic group associated with v, as defined above.

Proposition 9.3.3 *Let $u = \text{lcm}\{q^m - 1 \mid m|d, 0 < m < d\}$. Then v_λ divides u.*

Proof: We must show u is a scale: $x \equiv y \pmod{u}$ implies $\lambda_x = \lambda_y$. So assume $\lambda_x - \lambda_y \neq 0$, thus $t_{xy} = \gcd(\lambda_x - \lambda_y, d)$ is a non-zero divisor of d. If $x \equiv y \pmod{u}$, then every *non-zero* $q^{t_{ab}} - 1$, for distinct $a, b \in I_{n-1}$, divides u and hence also $x - y$. But for $a = x$, $b = y$ we now have $x \equiv y \pmod{q^{t_{xy}} - 1}$. Now by the definition of a λ-system, we have, see theorem 9.1.2, $\lambda_x = \lambda_y$. The contradiction yields the result.■

9.4 André Systems.

The following proposition introduces the original André systems in terms of generalized André systems.

Theorem 9.4.1 *Define the map*

$$\nu : I_{n-1} \to I_{q-1}$$
$$\nu(i) \equiv i \pmod{(q-1)}$$

and let $\mu : I_{q-1} \to I_d$ be an arbitrary map such that $\mu(0) = 0$. Then

1. *$\lambda = \mu\nu()$ is a λ-function defining a quasifield Q_λ called an André system. The v for an André system divides $q - 1$*

2. *Conversely, if a λ-system has v dividing $q - 1$ then it must be a generalized André system.*

3. In any André system $\lambda(x \circ y) = \lambda(xy)$. Hence the system is nearfield iff λ is a homomorphism from I_{n-1} to I_d.

Proof: If $i \equiv j \pmod{q^{t_{ij}} - 1}$ then certainly $i \equiv j \pmod{q - 1}$ and this implies $\lambda_i = \lambda_j$, by the definition of ν and μ, and now $t_{ij} = d$ so $i \equiv j \pmod{q^d - 1}$, and hence $i = j$. Thus an André system is a quasifield. Also if $i \equiv j \pmod{q - 1}$ then the defintion of an Andr'e system implies that $\lambda_i = \lambda_j$; but v is the least integer for which this holds. Thus v divides $q - 1$. The converse follows because v dividing $q - 1$ means that λ is constant on points differing by multiples of $q - 1$: so choose μ to be the common value of such additive cosets of $< q - 1 >$.
To check $\lambda(x \circ y) = \lambda(xy)$ in additive form we write $x = \omega^X$, $y = \omega^Y$ and now we need to show

$$\lambda(Xq^{\lambda_Y} + Y) \equiv \lambda(X + Y).$$

But $Xq^{\lambda_Y} + Y \equiv X + Y \pmod{q - 1}$ certainly holds, because $q \equiv 1 \pmod{q - 1}$, so the identity holds because the 'scale' v for λ divides $q - 1$. ■

9.5 Highest Prime-Power Divisors of $a - 1$ Dividing $a^d - 1$.

Let u be a prime dividing $a - 1$. The aim of this section is to consider the highest power of u that divides $a^n - 1$, where $n > 1$ is an integer. A lower bound follows by a simple induction:

Lemma 9.5.1 *If u^A divides $a - 1$ and u^B divides n then u^{A+B} divides $a^n - 1$.*

Proof: Write $n = u^B\delta$, where $\gcd(u, \delta) = 1$. Apply induction on B. Since $(a - 1)$ is a factor of $a^n - 1$ the desired result holds for $B = 0$. Assume $u^{A+B} \| a^n - 1$, when $B = b$. Then consider the next case $B = b + 1$ using:

$$a^{u^{b+1}\delta} - 1 = (a^{u^b\delta} - 1)\sum_{i=0}^{u-1} a^{u^b\delta i},$$

and now by the inductive hypothesis the term $(a^{u^b\delta} - 1)$ is divisible by u^{A+B} and the summation is $\equiv u \pmod{u}$ since each of the u terms involved in it are $\equiv 1 \pmod u$. Thus the lhs is divisible by u^{A+B}, when $B = b + 1$. The desired conclusion follows. ■

In the somewhat vacuous case, when $\gcd(n, u) = 1$, the lower bound above implies an exact value for the highest power of u dividing $a^n - 1$:

Corollary 9.5.2 *Suppose u is a prime divisor of $a - 1$ such that $u^\alpha \| a - 1$ and $u^\beta \| n$. Then: $u^{\alpha+\beta} | a^n - 1$, and if $\beta = 0$ then $u^{\alpha+\beta} \| a^n - 1$.*

We adopt the hypothesis of the corollary for the rest of the section; $u^r \| R$ means u^r is the highest power of the prime u dividing the integer R.

Our principal aim is to show that the corollary 9.5.2 holds in the general case when $u^\alpha > 2$ and β is arbitrary: thus the exact value of the highest power of u dividing $a^n - 1$ is the lower bound given in the corollary, unless $2 \| a - 1$, in which case the lower bound $u^{\alpha+\beta}$ is *not* sharp for $\beta > 0$. We verify this first.

Remark 9.5.3 *Suppose $2 \| a - 1$, and write $n = 2^\beta \delta$, so δ is odd. Then, for $\beta \geq 1$:*

$$a^n - 1 \equiv 0 \pmod{2^{\beta+2}}.$$

Proof: If $\beta = 1$ then

$$a^n - 1 = (a^{d/2} - 1)(a^{n/2} + 1) \equiv 0 \pmod 8,$$

as required. The general case follows by induction on β: assume the result holds when $2^\beta \| n$, and consider the next case where $n = 2^{2^{\beta+1}\delta}$, δ odd.

$$a^{2^{\beta+1}\delta} - 1 = \left(a^{2^\beta \delta} - 1\right)\left(a^{2^\beta \delta} + 1\right) \equiv 0 \pmod{2^{\beta+2}2},$$

by the inductive hypothesis, so the desired result follows. ■

Thus, the remark asserts that if $u = 2$ and $\alpha = 1$ then $u^{\alpha+\beta+1}$ divides $a^n - 1$, where $u^\beta \| n$. The rest of the section is concerned with showing that this does not happen in any other case, that is, we shall establish that:

$$u^{\alpha+\beta} \| a^n - 1 \Rightarrow u^\alpha = 2,$$

and this situation has been considered in remark 9.5.3 above.

We begin by noting that in all cases it is justifiable to assume $n = u^\beta$ whenever convenient:

Remark 9.5.4 *When $u^\beta \| n$ then $u^A \| a^n - 1$ iff $u^A \| a^{u^\beta} - 1$.*

Proof: Defining m so that $n = u^\beta m$, we have $\gcd(u,m) = 1$, and hence also

$$a^n - 1 = (a^{u^\beta} - 1)\sum_{i=0}^{m-1} a^{u^\beta i},$$

and since $a \equiv 1 \pmod u$ we now have

$$a^n - 1 = (a^{u^\beta} - 1)m,$$

yielding the desired result, since $\gcd(u,m) = 1$. ■

So to determine when $u^{\alpha+\beta} \| a^n - 1$, we need to consider its negation, the following condition:

$$u^{\alpha+\beta+1} | a^{u^\beta} - 1. \tag{9.2}$$

As mentioned earlier, the condition cannot hold when $\beta = 0$. Thus if the condition (9.2) ever holds, for some u^α, then there is a maximum integer $b \geq 1$ such that condition (9.2) fails for $\beta := b$ but holds for $\beta = b + 1$. We have seen already, in remark 9.5.3, that if $u^\alpha = 2$ then $b = 1$ can be chosen, and condition (9.2) holds for $\beta \geq 1$. In order to show that condition (9.2) does not hold in any other circumstance we essentially need to establish if it fails for a given β (which it always does when $\beta = 0$) then it cannot hold for the next β, unless, as we have seen, $u^\alpha = 2$.

Lemma 9.5.5 *Suppose that there is an integer $\beta \geq 0$ such that:*

$$a^{u^\beta} - 1 \not\equiv 0 \pmod{u^{\alpha+\beta+1}}. \tag{9.3}$$

$$a^{u^{\beta+1}} - 1 \equiv 0 \pmod{u^{\alpha+\beta+2}} \tag{9.4}$$

Then $\beta = 0$ and $u^\alpha = 2$.

Proof: Writing

$$a^{u^{\beta+1}} - 1 = \left(a^{u^\beta} - 1\right)\left(\sum_{i=0}^{u-1} a^{u^\beta i}\right),$$

we have by condition (9.4):

$$\left(a^{u^\beta} - 1\right)\left(\sum_{i=0}^{u-1} a^{u^\beta i}\right) \equiv 0 \pmod{u^{\alpha+\beta+2}}$$

and since by lemma 9.5.1 and condition (9.3)

$$u^{\alpha+\beta} \| a^{u^\beta} - 1,$$

we now have

$$\sum_{i=0}^{u-1} a^{u^\beta i} \equiv 0 \pmod{u^2} \tag{9.5}$$

and we also have from lemma 9.5.1 that for each i:

$$a^{u^\beta i} \equiv 1 \pmod{u^{\alpha+\beta}}, \tag{9.6}$$

and in particular:

$$\text{If } \alpha+\beta \geq 2 \text{ then: } a^{u^\beta i} \equiv 1 \pmod{u^2} \tag{9.7}$$

which combines with (9.5) to yield:

$$\text{If } \alpha+\beta \geq 2 \text{ then: } u \equiv 0 \pmod{u^2}, \tag{9.8}$$

which is a contradiction, unless $\alpha + \beta \leq 1$.
But since hypothesis $u|a-1$, we must now have $\alpha = 1$ and $\beta = 0$, and condition (9.3) holds, as remarked earlier. In view of our hypothesis that $u^\alpha > 2$ we now also have:

$$u^\alpha = u \text{ is an odd prime divisor of } a-1 \tag{9.9}$$

Moreover, the condition (9.4) reduces to

$$a^u - 1 \equiv 0 \pmod{u^3}. \tag{9.10}$$

and on applying (9.9) this yields

$$\sum_{i=0}^{u-1} a^i \equiv 0 \pmod{u^2}. \tag{9.11}$$

Moreover,

$$\begin{aligned} \sum_{i=0}^{u-1} a^i &= u + \sum_{i=1}^{u-1}(a^i - 1) \\ &= u + (a-1)\sum_{i=1}^{u-1}\sum_{j=1}^{i-1} a^j, \end{aligned}$$

and since $a-1 \equiv 0 \pmod u$ and $a^j \equiv 1 \pmod u$ we also have $(a-1)a^j \equiv (a-1)1 \pmod{u^2}$. Thus

$$\begin{aligned}\sum_{i=0}^{u-1} a^i &\equiv u + \sum_{i=1}^{u-1} i \pmod{u^2}, \\ &\equiv u + (a-1)\frac{u(u-1)}{2} \pmod{u^2}\end{aligned}$$

and since the LHS $\equiv 0 \pmod{u^2}$, by eqn (9.11), we now have:

$$1 + \frac{(a-1)(u-1)}{2} \pmod u,$$

but since the prime u is an odd divisor $a-1$ we have a contradiction. ∎
Combining lemma 9.5.5 with remark 9.5.3 yields, for $u^\alpha > 2$, $u^{\alpha+\beta}$ is the highest power of u dividing $a^n - 1$

Theorem 9.5.6 *Suppose $a > 1$ and $n \geq 1$ are integers and u is a prime divisor of $a-1$ such that $u^\alpha \| a-1$ and $u^\beta \| n$.*

1. *If $u^\alpha > 2$ or $\beta = 0$ then*
$$u^{\alpha+\beta} \| a^n - 1.$$
2. *If $u^\alpha = 2$ and $\beta \geq 1$ then*
$$u^{\alpha+\beta+1} | a^n - 1.$$

Our next objective is to apply the theorem above to show that under its hypothesis $a^k - 1/a - 1$ ranges over all residues mod$N$, as k varies. This is crucial in defining the Dickson nearfields.

Lemma 9.5.7 *Let $a > 1$ and $N > 1$ be integers such that:*

1. *every prime divisor of N divides $a-1$; and*
2. *if $a \equiv 3 \pmod 4$ then $N \not\equiv 0 \pmod 4$.*

Then $a^N - 1 \not\equiv 0 \pmod{N(a-1)}$ for $1 \leq n < N$.

Proof: To obtain a contradiction assume that for some $n \in [1, N-1]$:

$$a^n - 1 \equiv 0 \pmod{N(a-1)}. \tag{9.1}$$

Since $n < N$, there is at least one prime divisor u of N such that for some integer $b \geq 0$, $u^b \| n$ and $u^{b+1} | N$. By theorem 9.5.6, $a^n - 1$ is divisible by $u^{\alpha+\beta}$, and this is the highest power of u dividing $a^n - 1$, unless $u^\alpha = 2$. So for $u^\alpha > 2$, $u^{\alpha+b} \| a^n - 1$, contrary to eqn (9.1). Thus we may further assume that $u^\alpha = 2$, So 2^{b+1} divides N, and this contradicts our hypothesis that $N \not\equiv 0 \pmod 4$, when $2 \| a - 1$, unless $b = 0$. But in this case theorem 9.5.6 still implies $u^{\alpha+b} \| a^n - 1$, again contradicting eqn (9.1). ∎
We now obtain the desired result, that $a^k - 1/a - 1$ ranges over the residues mod$n$ as k ranges over $1 \ldots n$.

Proposition 9.5.8 *Let $a > 1$ and $n > 1$ be integers such that:*

1. *every prime divisor of n divides $a - 1$; and*

2. *if $a \equiv 3 \pmod 4$ then $n \not\equiv 0 \pmod 4$.*

Then the n distinct integers:

$$1, \frac{a^2-1}{a-1}, \frac{a^3-1}{a-1}, \ldots, \frac{a^n-1}{a-1},$$

constitute a complete set of n residues mod$n$. *In particular, $a^n - 1/a - 1 \equiv 0 \pmod n$.*

Proof: The difference of two distinct terms of the above list, associated with $i > j$, yields:

$$\begin{aligned} \frac{a^i-1}{a-1} &\equiv \frac{a^j-1}{a-1} \pmod n \\ \Rightarrow a^j \frac{a^{i-j}-1}{a-1} &\equiv 0 \pmod n \\ \Rightarrow \frac{a^{i-j}-1}{a-1} &\equiv 0 \pmod n, \end{aligned}$$

contradicting lemma 9.5.7. Thus each of the n listed terms is a distinct residue mod$n$. Moreover, $a^n - 1/a - 1 \equiv 0 \pmod n$ follows directly from theorem 9.5.6. ∎

9.6 Dickson Nearfields.

Let $F = GF(q^n)$, and assume (q, n) is a Dickson pair: so the prime divisors of n divide $q-1$, and if $q \equiv 3 \pmod 4$ then $n \not\equiv 0 \pmod 4$.

Hence $(q^n - 1)/n$ is an integer because the maximum prime-power divisors of n divide $q^n - 1$. So the cyclic group F^* has a unique subgroup N of order $q^n - 1/n$, and on applying proposition 9.5.8, to the cyclic group F^*/N^* of order n, we may write F^* as a union of cosets of N in the form:

$$F^* = \theta N \bigcup \theta^{\frac{q^2-1}{q-1}} N \bigcup \theta^{\frac{q^3-1}{q-1}} N \bigcup \ldots \bigcup \theta^{\frac{q^n-1}{q-1}} N,$$

where $\theta \in F^* - N$ is such that θN generates the cyclic group F^*/N.

Lemma 9.6.1 *Suppose $b, c \in F^*$ are given by:*

$$\begin{aligned} b &= \theta^{\frac{q^\beta-1}{q-1}} y, \exists y \in N; \\ c &= \theta^{\frac{q^\gamma-1}{q-1}} z, \exists z \in N. \end{aligned}$$

Then

$$b^{q^\gamma} c \in \theta^{\frac{q^{(\beta+\gamma) \bmod n}-1}{q-1}} N.$$

Proof:

$$\begin{aligned} b^{q^\gamma} c &= (\theta^{\frac{q^\beta-1}{q-1}} y)^{q^\gamma} \theta^{\frac{q^\gamma-1}{q-1}} z \\ &= \theta^{\frac{q^{\beta+\gamma}-q^\gamma}{q-1}} y^{q^\gamma} \theta^{\frac{q^\gamma-1}{q-1}} z \\ &= \theta^{\frac{q^{\beta+\gamma}-q^\gamma+q^\gamma-1}{q-1}} y^{q^\gamma} z, \\ &\in \theta^{\frac{q^{\beta+\gamma}-1}{q-1}} N, \text{by invariance of } N \text{ under group homomorphisms}, \\ &= \theta^{\frac{q^{(\beta+\gamma) \bmod n}-1}{q-1}} N, \end{aligned}$$

the desired result. ∎

Definition 9.6.2 (Dickson Nearfields.) *Let (q, n) be a Dickson pair. Then for $m \in \theta^{\frac{q^i-1}{q-1}} N$, define the field automorphism $\lambda(x) \in \mathrm{Gal}(GF(q^n)/GF(q))$ by:*

$$\lambda(m) : x \mapsto x^{q^i},\ i \in \{1, 2 \ldots, n\},$$

and the product $(F, \circ)$, $f = GF(q^n)$, by $x \circ 0 = 0$, for $x \in F$ and:

$$x \circ m = \begin{cases} x^{\lambda(m)}m & \text{if } m \in F^* \\ 0 & \text{if } m = 0 \end{cases}$$

We call all any such $(F, +, \circ)$ a Dickson nearfield, associated with λ and θ.

It is a tautology to claim that any Dickson nearfield is a generalized André plane. However, we have yet to establish that $(F, +, \circ)$ is always a nearfield. This is our goal for the rest of the section, so we assume the notation of definition 9.6.2. To establish that the product $\circ$ yields a quasifield essentially involves showing that 'slopemaps' of the non-identity elements of F^*, relative to $\circ$, are semiregular on F^*.

Lemma 9.6.3 *Suppose: $x \circ m = x$ for some $x, m \in F^*$. Then $m = 1$.*

Proof: Suppose $x \circ m = x$. Writing $x = \theta^{\frac{q^j-1}{q-1}}$ and $y = \theta^{\frac{q^i-1}{q-1}}$, where $i, j \in [1, n]$, we have

$$\begin{aligned}
\left(\theta^{\frac{q^j-1}{q-1}}\right)^{q^i} \theta^{\frac{q^i-1}{q-1}} &\equiv \theta^{\frac{q^j-1}{q-1}} \pmod N, \\
\text{so } \theta^{\frac{q^{j+i}-1}{q-1}} &\equiv \theta^{\frac{q^j-1}{q-1}} \pmod N, \\
\text{so } \theta^{\frac{q^{j+i}-q^j}{q-1}} &\in N, \\
\text{so } \left(\theta^{\frac{q^i-1}{q-1}}\right)^{q^j} &\in N, \\
\text{so } \theta^{\frac{q^i-1}{q-1}} &\in N,
\end{aligned}$$

yielding $i = n$. So $1 = x \circ m = xm$, and we have $m = 1$ as required. ∎

To show that $(F^*, \circ)$ is a group we first note that it is an associative binary system with identity. The proof depends on extensive tacit use of the 'product' computed in lemma 9.6.1.

Lemma 9.6.4 *$(F^*, \circ)$ is an associative binary system with identity $1 \in F$.*

Proof: Since $a \circ b \in F^*$ whenever $a, b \in F^*$ we have a binary system, and the multiplicative identity of F^* is the identity for $(F^*, \circ)$ by the definition of $\circ$. To show $\circ$ is associative, we represent $x, y, z \in F^*$ in the form:

$$\begin{aligned}
x &= \theta^{\frac{q^a-1}{q-1}} n_y, \exists n_x \in N; \\
y &= \theta^{\frac{q^b-1}{q-1}} n_y, \exists n_y \in N; \\
z &= \theta^{\frac{q^c-1}{q-1}} n_z, \exists n_z \in N,
\end{aligned}$$

where $a, b, c \in \{1 \ldots, n\}$. Applying lemma 9.6.1 repeatedly to the definition of $\circ$, we have

$$\begin{aligned}
x \circ (y \circ z) &= \left(\theta^{\frac{q^a-1}{q-1}} n_x\right) \circ (y \circ z) \\
&= \left(\theta^{\frac{q^a-1}{q-1}} n_x\right)^{q^{(b+c) \bmod n}} \theta^{\frac{q^{(b+c) \bmod n}-1}{q-1}} n_y^{q^c} n_z \\
&= \theta^{\frac{q^{(a+b+c) \bmod n} - q^{(b+c) \bmod n}}{q-1}} \theta^{\frac{q^{(b+c) \bmod n}-1}{q-1}} n_x^{q^{(b+c) \bmod n}} n_y^{q^c} n_z \\
&= \frac{\theta^{q^{(a+b+c) \bmod n}-1}}{q-1} n_x^{q^{(b+c) \bmod n}} n_y^{q^c} n_z,
\end{aligned}$$

and similarly:

$$\begin{aligned}
(x \circ y) \circ z &= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right) \circ z \\
&= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right) \circ \theta^{\frac{q^c-1}{q-1}} n_z \\
&= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right)^{q^c} \theta^{\frac{q^c-1}{q-1}} n_z \\
&= \left(\theta^{\frac{q^{(a+b+c) \bmod n}-q^c}{q-1}} n_x^{q^{(b+c) \bmod n}} n_y^{q^c}\right) \theta^{\frac{q^c-1}{q-1}} n_z \\
&= \theta^{\frac{q^{(a+b+c) \bmod n}-1}{q-1}} n_x^{q^b+q^c} n_y^{q^c} n_z,
\end{aligned}$$

and the associativity of $\circ$ follows on comparing the values of $(x \circ y) \circ z$ and $x \circ (y \circ z)$ obtained above. ■

The maps $T_m : x \mapsto x \circ m$, for $m \in F^*$, are obviously in $GL(F, +)$ and lemma 9.6.4 above implies that such maps are closed under composition, thus:

$$\tau = \{T_m : x \mapsto x \circ m \in GL(F, +) \mid m \in F^*\}$$

is a subgroup of $GL(F, +)$, and by lemma 9.6.3 every T_m, $m \in F^* - \{1\}$, is semiregular on F^*. This forces the difference between any two distinct members of τ to be a non-singular map of $(F, +)$, since otherwise a non-identity element of τ would fix some element of F^*. Thus τ together with the zeromap forms a spreadset that is multiplicatively closed. Now by this alone (or alternatively by lemma 9.6.4 above) $(F, +, \circ)$ is a nearfield. Thus we have established:

Theorem 9.6.5 *Given a Dickson pair* (q, n) *and* $(F, +, \circ)$ *be as in definition 9.6.2. Then* $(F, +, \circ)$ *is a generalized André system relative to the given* λ *that is associative. Such generalized André systems are called Dickson nearfields.*