Nearfields

Definition of nearfield and commutativity. By definition, $(N, +, \cdot, 0, 1)$ is a nearfield if $(N, +, 0)$ and $(N^*, \cdot, 1)$ are groups, $x(y+z) = xy+xz$ for all $x, y, z \in N$, and the 2-element structure with $xy = y$ is avoided. To avoid it, it may be assumed, e.g., that $0 \cdot 1 = 0$.

In every nearfield $x+y = y+x$, for every x and y. The proof of commutativity is nontrivial in the general case. In finite case the commutativity follows from the fact that finite nearfields are quasifields. Another proof of commutativity in the finite case relies upon the fact that $x \mapsto cx$ is an automorphism of $(N, +, 0)$ for every $c \in N^*$. This means that $c = c \cdot 1$ is an automorphic image of the element 1. Hence all elements of N^* are of the same order. This is possible if and only if each element of N^* is of a prime order p. Therefore $(N, +, 0)$ is a p-group. A p-group always contains a nontrivial center. A nontrivial element of this center is an automorphic image of 1. Hence 1 belongs to the center. Each element of N^* is thus central. This proves that *the additive group of a finite nearfield is an elementary abelian p-group, p a prime.*

Further on the additive group of $(N, +)$ will always be considered to be commutative.

Opposite elements in a nearfield. As observed earlier, $0a = a0 = 0$ and $a(-b) = -ab$ in every nearfield N. In a nearfield $a + b = b + a$. Here we shall show that $(-a)b = -ab$ for all $a, b \in N$.

Lemma. An element $a \in N$ fulfils $a^2 = 1$ if and only if $a = \pm 1$.

Proof. $(-1)(-1) = -(-1) = 1$. If $a^2 = 1$, then $a(a+1) = a^2 + a = 1 + a = 1(a+1)$. If $a + 1 \neq 0$, then $a = 1$. If $a + 1 = 0$, then $a = -1$. □

Lemma. Every $a \in N$ fulfils $(-1)a = -a$.

Proof. This is clear if $a = 0$. Assume $a \neq 0$ and consider $b \in N^*$ such that $ab = 1$. Then $ba = 1$ and $(a \cdot (-1) \cdot b)(a \cdot (-1) \cdot b) = a \cdot (-1) \cdot (-1) \cdot b = a \cdot b = 1$. By the lemma, $a \cdot (-1) \cdot b = \pm 1$. If $a \cdot (-1) \cdot b = 1 = ab$, then $-a = a(-1) = a$. In such a case $0 = a + a$ and $0 = b(a + a) = ba + ba = 2$. That implies $-1 = 1$. Hence $a \cdot (-1) \cdot b = -1$ in every case. This yields $a \cdot (-1) = (-1)a$, by multiplying by a on the right. Hence $(-1)a = a(-1) = -a$. □

To finish note that $-ab = (-1)ab = (-1)a \cdot b = (-a)b$, for all $a, b \in N$.

Few notions from permutation groups. Let G be a permutation group upon Ω. Recall that $G_\alpha = \{g \in G;\ g(\alpha) = \alpha\}$, for all $\alpha \in \Omega$. The group is transitive if for all $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $g(\alpha) = \beta$. Note that for G to be transitive it suffices that there exists $\alpha \in \Omega$ such that for each $\beta \in \Omega$ there exists $g \in G$ such that $g(\alpha) = \beta$.

The group G is said to be 2-*transitive* if for all $\alpha, \beta, \gamma, \delta \in \Omega$ such that $\alpha \neq \beta$ and $\gamma \neq \delta$ there exists $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$. Note that for G to be 2-transitive it suffices that there exist $\alpha, \beta \in \Omega$, $\alpha \neq \beta$, such that for all $\gamma, \delta \in \Omega$, $\gamma \neq \delta$, there exists $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$.

If G is 2-transitive, and there exists only one $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$, then g is said to be *sharply* 2-*transitive*.

Note that the similar notion of sharp 1-transitivity coincides with the notion of a regular permutation group. Note also that a 2-transitive permutation group is sharply 2-transitive if and only if $G_{\alpha,\beta} = 1$, whenever $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$.

The permutation group G is said to be a *Frobenius group* if it is transitive, but not regular, and fulfils $G_{\alpha,\beta} = 1$ whenever $\alpha, \beta \in \Omega$ and $\alpha \neq \beta$. By a well known

theorem a finite Frobenius group contains a normal subgroup that consists of the identity mapping and of all mappings $g \in G$ such that $g(\alpha) = \alpha$ for no $\alpha \in \Omega$ (the regular permutations of G). This subgroup is normal and is called the *Frobenius kernel*. Each sharply 2-transitive group is a Frobenius group. The converse is not true.

Affine mappings of a nearfield. Let N be a nearfield. Denote by $\mathrm{Aff}(N)$ the set of all mappings $x \mapsto ax + b$, where $a \in N^*$ and $b \in N$. The set $\mathrm{Aff}(N)$ forms a group and this group is sharply 2-transitive.

As explained above, to prove this it suffices to show that for $c, d \in N$, $c \neq d$, there exist a unique affine mapping $x \mapsto ax + b$ that sends 0 upon c and 1 upon d. These assumptions mean that $c = a0 + b = b$ and $d = a1 + b = a + b$. Setting $a = d - c$ and $b = c$ thus does the job.

Finite nearfields are equivalent to sharply 2-transitive groups. Let G be a sharply 2-transitive permutation group upon a finite set N. Choose an element of N and denote it by 0. The Frobenius kernel of G is a regular group upon N. Hence N may be considered as a group $(N, +, 0)$, where $+$ is defined in such a way that the Frobenius kernel coincides with the set of left translations L_a, $a \in N$. (The way how to define $+$ is described in the passage about regular group.)

The Frobenius kernel is a normal subgroup of G. Hence if $g \in G$, then for each $a \in N$ there exists $b \in N$ such that $gL_ag^{-1} = L_b$. If $g \in G_0$, then $gL_a(0) = g(a) = b = L_b(0) = L_bg(0)$. Thus $gL_ag^{-1} = L_{g(a)}$ for each $g \in G_0$ and $a \in N$.

Choose a nonzero element of N and denote it by 1. Define multiplication upon N so that $0a = 0$ and $ab = \varphi_a(b)$ whenever $a, b \in N$, $a \neq 0$ and φ_a is the unique element of G_0 that sends 1 upon a. Put $N^* = N \setminus \{0\}$ and denote by φ_a^* the restriction of φ_a to N^*. By the definition $ab = \varphi_a^*(b)$ for all $a, b \in N^*$. The group G_0 consists of all φ_a, $a \in N^*$. Permutations φ_a^* coincide with left translations of $(N^*, \cdot)$. That makes $(N^*, \cdot)$ a group. Note that $\cdot$ is defined in accordance with the general procedure of deriving an abstract group from a regular group. The neutral element of N^* is equal to 1 since $\varphi_1 = \mathrm{id}_N$.

The left distributive law $a(b+c) = ab+ac$ clearly holds if $a = 0$. Assume $a \in N^*$. Then $a(b + c) = \varphi_a L_b(c) = L_{\varphi_a(b)}\varphi_a(c) = L_{ab}(ac) = ab + ac$.

Dickson nearfields. Finite nearfields are thus equivalent to sharply 2-transitive permutation groups. All such groups are known. Their classification belongs to Zassenhaus. Here it will not be discussed. The simplest example of *proper nearfields* (that is nearfields that do not satisfy the right distributive law) are Dickson nearfields.

A *Dickson nearfield* is obtained by replacing the multiplication $\cdot$ of $\mathbb{F}_{q^2}$ (the finite field of order q^2), q odd, by multiplication $\circ$ that is defined as follows:

$$a \circ b = \begin{cases} ab & \text{if } a \text{ is a square;} \\ ab^q & \text{if } a \text{ is a nonsquare.} \end{cases}$$

Exercise. Show that $(\mathbb{F}_{q^2}, +, \circ, 0, 1)$ is a nearfield, for any $q > 1$ that is a power of odd prime.

Exercise. The smallest order of a Dickson nearfield (and, in fact, of any proper nearfield) is 9. Prove that $(\mathbb{F}_9^*, \circ)$ is isomorphic to Q_8, the group of quaternions.

Quasigroups from nearfields. Let $(N,+,\cdot,0,1)$ be a nearfield. Choose an element $c \in N$, $c \notin \{0,1\}$, and define a binary operation $*_c$ upon N by

$$x *_c y = x + (y-x)c \text{ for all } x,y \in N.$$

Suppose that $a,b \in N$.

$$\begin{aligned} a *_c y = b &\Leftrightarrow a + (y-a)c = b \Leftrightarrow y - a = (-a+b)c^{-1}, \text{ and} \\ x *_c a = b &\Leftrightarrow x + (a-x)c = b \Leftrightarrow (-a+x) + (a-x)(c) = -a+b \\ &\Leftrightarrow (a-x)(-1) + (a-x)(c) = -a+b \Leftrightarrow (a-x)(-1+c) = -a+b \\ &\Leftrightarrow a - x = (-a+b)(-1+c)^{-1}. \end{aligned}$$

Both equations thus possess a unique solution. That makes $(N,*_c)$ a quasigroup. This quasigroup is idempotent since $a *_c a = a + (a-a)c = a + 0c = a$.

Theorem. *Let N be a nearfield, $c \in N$, $c \notin \{0,1\}$. Then* $\mathrm{Aff}(N) \leq \mathrm{Aut}(N,*_c)$.

Proof. The group $\mathrm{Aff}(N)$ is generated by mappings $x \mapsto x+v$, $v \in N$, and mappings $x \mapsto ux$, $u \in N^*$. The proof uses the commutativity of $+$. If $x,y \in N$, then $(x+v) *_c (y+v) = x + (y-x)c + v = (x *_c y) + v$ since $(y+v) - (x+v) = y - x$. Furthermore, $ux *_c uy = ux + (uy - ux)c = ux + u(y-x)c = u(x + (y-x)c) = u(x *_c y)$. □

A lemma of general nature. *Let $(Q,*)$ be an idempotent quasigroup. If $x,y \in Q$ are such that (x,x,y) or (y,x,x) is an associative triple, then $x = y$.*

Proof. Assume $x * (x * y) = (x * x) * y$. Since $(x * x) * y = x * y$ there must be $x * y = y = y * y$. Thus $x = y$. □

Flexibility. A binary operation $\cdot$ is said to be *flexible* if it fulfils the *flexible law* $xy \cdot x = x \cdot yx$.

Let N be a nearfield, and $c \in N \setminus \{0,1\}$. The aim now is to prove that $*_c$ *is flexible if and only if* $c(1-c) = (1-c)c$. *If* $c(1-c) \neq (1-c)c$ *then* (a,b,a) *is never associative if* $a,b \in N$ *and* $a \neq b$.

First note if $(Q,\cdot)$ is a quasigroup and $\alpha \in \mathrm{Aut}(Q)$, then $(a,b,c) \in Q^3$ is associative if and only if $(\alpha(a),\alpha(b),\alpha(c))$ is associative. This is because $\alpha(a)\alpha(b) \cdot \alpha(c) = \alpha(ab \cdot c)$ and $\alpha(a) \cdot \alpha(b)\alpha(c) = \alpha(a \cdot bc)$.

Consider $a,b \in N$, $a \neq b$. Since $\mathrm{Aff}(N)$ is 2-transitive, there exists $\alpha \in \mathrm{Aff}(N)$ such that $\alpha(0) = a$ and $\alpha(1) = b$. Recall that $\mathrm{Aff}(N) \leq \mathrm{Aut}(N,*_c)$. This means that (a,b,c) is associative if and only if $(0,1,0)$ is associative.

Plugging $x = 0$ into $x *_c y = x + (y-x)c$ gives $0 *_c y = yc$. Furthermore, $x *_c 0 = x + (-x)c = x1 + x(-c) = x(1-c)$. Hence

$$\begin{aligned} &0 *_c (1 *_c 0) = (1 *_c 0)c = (1-c)c, \text{ and} \\ &(0 *_c 1) *_c 0 = c *_c 0 = c(1-c). \end{aligned}$$

Flexibility in Dickson nearfields. The operation of the Dickson nearfield upon $\mathbb{F}_{q^2}$ is denoted by $\circ$. For $i,j \in \{0,1\}$ set $i = 0$ if c is square and $i = 1$ if it is a nonsquare. Similarly set $j = 0$ if $1-c$ is a square, and $j = 1$ othewise. Then

ij	00	01	10	11
$c \circ (1-c)$	$c(1-c)$	$c(1-c)$	$c(1-c)^q$	$c(1-c)^q = c - c^{q+1}$
$(1-c) \circ c$	$c(1-c)$	$c^q(1-c)$	$c(1-c)$	$c^q(1-c) = c^q - c^{q+1}$

The table shows that if c is a nonsquare or $1-c$ is a nonsquare, then $c \circ (1-c) = (1-c) \circ c$ implies $c = c^q$ or $1-c = (1-c)^q$. Now, $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^2}$ that consists of all $a \in \mathbb{F}_{q^2}$ that fulfil $a^q = a$. Since each element of $\mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$, the equality $c \circ (1-c) = (1-c) \circ c$ holds if and only if both c and $1-c$ are squares.

In other words, $(\mathbb{F}_{q^2}, *_c)$ is flexible if and only if both c and $1-c$ are squares, whenever $c \in \mathbb{F}_{q^2}$ and $c \notin \{0,1\}$.

Maximal nonassociativity via nearfields. Let c be an element of a nearfield N such that $c(1-c) \neq (1-c)c$. If (x,y,z) is a nondiagonal associative triple in $(N, *_c)$, then the elements x, y and z have to be pairwise distinct, by the results above.

Since there exists $\alpha \in \mathrm{Aff}(N) \leq \mathrm{Aut}(N, *_c)$ such that $\alpha(0) = x$ and $\alpha(1) = y$, the quasigroup $(N, *_c)$ **is maximally nonassociative if and only if** $(0 *_c 1) *_c z \neq 0 *_c (1 *_c z)$ **for every** $z \in N$, $z \notin \{0,1\}$. Note that

$$(0 *_c 1) *_c z = c + (z-c)c \text{ and } 0 *_c (1 *_c z) = (1 + (z-1)c)c.$$

Maximal nonassociativity via Dickson nearfields. It may be proved that for each odd $q > 1$, q a power of an odd prime, there exists $c \in \mathbb{F}_{q^2}$ such that the quasigroup $(\mathbb{F}_{q^2}, *_c)$ is maximally nonassociative. The proof is nonconstructive—the idea is to estimate the number of $c \in \mathbb{F}_{q^2}$, $c \notin \{0,1\}$, for which there exists a nondiagonal associative triple, and show that this number is less than $q^2 - 2$.

The case of $q = 3$ is easy to verify by hand. It turns out that $(\mathbb{F}_9, *_c)$ is maximally nonassociative whenever $c \notin \mathbb{F}_3$. Furthermore, if $c, d \in \mathbb{F}_9 \setminus \mathbb{F}_3$, then $(\mathbb{F}_9, *_c) \cong (\mathbb{F}_9, *_d)$.

The weighted average. Consider now the quasigroup $(F, *_c)$ in the case when F is a field (or, more generally, a division ring), and $c \notin \{0,1\}$. The operation

$$x *_c y = x + (y-x)c = x(1-c) + yc$$

is known as the *weighted average*. It fulfils the *medial* law $xy \cdot uv = xu \cdot yv$. That may easily be verified directly. Another way how to prove it is to use a construction below. The connection to the construction is by the fact that both $x \mapsto xc$ and $x \mapsto x(1-c)$ are automorphisms of the group $(F, +, 0)$.

Another name for the medial law is the *entropic* law.

A construction. Let $(G, +)$ be an Abelian group, and let α and β be commuting automorphisms of $(G, +)$ (thus $\alpha\beta = \beta\alpha$). Furthermore, let c be an element of G. For $x, y \in G$ set

$$x * y = \alpha(x) + \beta(y) + c.$$

Then $(G, *)$ is quasigroup isotopic to $(G, +)$. If $x, y, u, v \in G$, then

$$\begin{aligned}(x * y) * (u * v) &= (\alpha(x) + \beta(y) + c) * (\alpha(u) + \beta(v) + c) \\ &= \alpha^2(x) + \alpha\beta(y) + \beta\alpha(u) + \beta^2(v) + \alpha(c) + \beta(c) + c \\ &= \alpha^2(x) + \alpha\beta(u) + \beta\alpha(y) + \beta^2(v) + \alpha(c) + \beta(c) + c \\ &= (x * u) * (y * v).\end{aligned}$$

Note that if $c = 0$ and $\alpha + \beta = \mathrm{id}_G$, then $x * x = x$. This is the case of the weighted average. Idempotent medial quasigroups are flexible. Indeed if $(Q, \cdot)$ is such a quasigroup, then $x \cdot yx = xx \cdot yx = xy \cdot xx = xy \cdot x$.

Toyoda theorem. *Let $(Q, *)$ be a medial quasigroup. Then Q may be equipped with the structure of an abelian group in such a way that there exist $\alpha, \beta \in \mathrm{Aut}(Q, +)$ and $c \in Q$ that fulfil $\alpha\beta = \beta\alpha$ and $x * y = \alpha(x) + \beta(y) + c$, for all $x, y \in Q$.*

The proof of Toyoda theorem takes about one page. One of the methods is to use properties of autotopisms.