INTRODUCING QUASIFIELDS

Incidence geometries. To understand the concept of dualization in line systems it seems useful to start with an abstract notion of incidence geometry. The main idea is that the relation 'point p is upon a line ℓ ' is read as 'point p is incident to line ℓ ', where the incidence is now expressed by a relation $\varepsilon \subseteq P \times L$, with P being the set of *points* and L the set of *lines*. This is an abstract approach in the sense that no other interaction between P and L is assumed but via the relation ε . Such systems are called (abstract) *incidence geometries*.

A definition of a 3-net in this context may be as follows: Let \parallel be an equivalence upon L, with classes L_1 , L_2 and L_3 . The incidence geometry (P, L) is called a 3-net if

$$\forall x \in L \ \forall p \in P \ \exists ! \ y \in L \text{ such that } x \parallel y \text{ and } p \in y; \text{ and}$$
(A1)

 $\forall x, y \in L \colon x \not\parallel y \implies \exists ! p \in P \text{ such that } p \in x \text{ and } p \in y.$ (A2)

The definition of a 3-net as done before can be obtained from the definition above by replacing $y \in L$ with the set $\ell_y = \{p \in P; p \in y\}$, and the relation $p \in y$ by $p \in \ell_y$. Note that the definition of a 3-net requires that the classes of \parallel are linearly ordered (i.e., (L_1, L_2, L_3) .)

Nets and affine planes. The definition of a 3-net may be generalized to a definition of a k-net, $k \ge 3$, by requiring that the number of classes of \parallel is equal to k. Again, the set of parallel classes—which often are called *pencils*—is supposed to be linearly ordered.

Let us now drop the requirement of the linear ordering of classes of \parallel and consider an incidence geometry defined by (A1), (A2) and

$$\forall p, q \in P \colon p \neq q \Rightarrow \exists ! y \in L \text{ such that } p \in y \text{ and } q \in y.$$
 (A3)

This may be interpreted by saying that any two points are connected by a unique line. (The requirement of uniqueness may be dropped since by (A1) and (A2) there cannot exist two distinct lines that would connect the points p and q, $p \neq q$.)

A system fulfilling (A1), (A2) and (A3) is said to be an *affine plane* if the equivalence \parallel contains has at least three classes. (Axiomatizations of affine planes usually achieve the latter requirement by stipulating that there exist three points that are not collinear.)

For the sake of completeness let it be remarked that the usual way how an affine plane is defined is to take as axioms (A1), (A3) and the existence of three noncollinear points, under the assumption that $x \parallel y$ if and only if either x = y, or there exists no $p \in P$ with $p \in x$ and $p \in y$ (i.e., $x \cap y = \emptyset$). With such a definition it is straightforward to prove first that \parallel is an equivalence on L, and then to derive (A2) from (A3).

Collineations. A collineation of an incidence geometry (P, L, ε) is a pair (α, β) such that α permutes P, β permutes L and

$$p \in x \Leftrightarrow \alpha(p) \in \beta(x), \text{ for all } (p, x) \in P \times L.$$

To see how to connect this notion of collineation with a standard definition of collineation of a line system (i.e., a system in which lines are considered as sets of points) let us first discuss a certain property of incidence geometries that is usually assumed to be true, and that will be assumed to be true from here on when an incidence geometry will be discussed.

For each $y \in L$ put $\ell_y = \{p \in P; p \in y\}$. For each $p \in P$ put $c_p = \{y \in L; p \in y\}$ (the letter *c* refers to lines *concurrent* to *p*. The property mentioned above states that

 $\mathbf{2}$

$$\forall x, y \in L \ (x = y \Leftrightarrow \ell_x = \ell_y) \text{ and } \forall p, q \in P \ (p = q \Leftrightarrow c_p = c_q).$$

In other words a line is determined completely by points incident to the line, and a point is determined completely by lines passing through the point. With this condition fufilled an incidence geometry may be turned into a system of lines $\mathcal{L} = \{\ell_y; y \in L\}$, where $p \in x \Leftrightarrow p \in \ell_y$.

It seems natural to define a collineation of a system of lines as a permutation of points such that a line is mapped upon a line. With an additional condition (like finiteness of the set, or the existence and uniqueness of a line passing through two points) this condition implies that the preimage of a line is a line. However, in general the latter property has to be considered as a part of definition. A collineation γ of a system of lines thus is a permutation of points such that $\gamma(\ell)$ and $\gamma^{-1}(\ell)$ is a line whenever ℓ is a line.

To see that both definitions of collineation coincide let us show that if (α, β) is a collineation of (P, L), then α is collineation of the system of lines $\{\ell_y; y \in L\}$, and that if γ is a collineation of such a system of lines, then there exists β such that (γ, β) is a collineation of (P, L).

Proof. The first step is to prove that if (α, β) is a collineation, then $\alpha(\ell_y) = \ell_{\beta(y)}$. This is true since $\alpha(p) \in \alpha(\ell_y) \Leftrightarrow p \in \ell_y \Leftrightarrow p \in y \Leftrightarrow \alpha(p) \in \beta(y) \Leftrightarrow \alpha(p) \in \ell_{\beta(y)}$, for all $(p, y) \in (P, L)$. For the converse direction assume that (P, L) is an incidence geometry and γ is a collineation of the line system $\{\ell_y; y \in L\}$. A line ℓ_y determines the element $y \in L$ completely. Hence there exists a permutation β of L such that $\gamma(\ell_y) = \ell_{\beta(y)}$. Now, $p \in y \Leftrightarrow p \in \ell_y \Leftrightarrow \gamma(p) \in \gamma(\ell_y) \Leftrightarrow \gamma(p) \in \ell_{\beta(y)} \Leftrightarrow \gamma(p) \in \beta(y)$.

The notion of collineation need not be used only for permutations of $P \times L$. A collineation $(P, L, \varepsilon) \to (P', L', \varepsilon')$ is a pair (α, β) such that α is a bijection $P \to P'$, β is a bijection $L \to L'$ and $p \varepsilon x \Leftrightarrow \alpha(p) \varepsilon' \beta(x)$. In terms of systems of lines γ is a bijection of points that both γ and γ^{-1} map lines upon lines.

Dual geometries and transversal designs. The *dual* geometry of (P, L, ε) is the geometry (L, P, ε') , where $p\varepsilon x \Leftrightarrow x\varepsilon' p$. Let us consider axioms (A1) and (A2) after dualization:

 $\forall p \in P \ \forall x \in L \ \exists ! q \in P \text{ such that } p \parallel q \text{ and } q \in x; \text{ and}$ (A1')

$$\forall p, q \in P \colon p \not| q \Rightarrow \exists ! x \in L \text{ such that } p \in x \text{ and } q \in x.$$
 (A2')

Consider a system fulfilling (A1') and (A2'). The equivalence \parallel is now an equivalence of points. Classes of \parallel are called *groups* (no connection to the algebraic notion of a group). Lines will be called *blocks*.

(A1') states that each block passes through exactly one point of a group and (A2') states that two points from distinct groups belong to exactly one block. A system of lines fulfilling these axioms is called a transversal design, provided that the number of groups is at least 3. If this number is equal to k, then the system is called a transversal k-design.

Groups of a transversal k-design are of the same size and this size is equal to the number of blocks passing through a point. Furthermore, each block is of size k. This is easy to prove. However, the proof may be omitted since the statement is a consequence of the fact that transversal k-designs dualize k-nets (with the exception that groups are not required to be linearly ordered).

The order of a transversal design is the number of points in a group. Transversal k-designs of order n are sometimes denoted as TD(k, n).

Counting and affine planes. Let us have a k-net of a finite order n. (The order is the number of points upon a line, and this is equal to the number of lines in a pencil.)

The number of 2-elements sets $\{a, b\}$ such that a and b are points of the net and there exists a line ℓ (which is unique) that passes through both a and b is equal to

'# pencils' · '# lines in a pencil' · '# of pairs upon a line' = $kn\binom{n}{2} = \frac{kn^2(n-1)}{2}$.

Number of all pairs of points in the net is

$$\binom{n^2}{2} = \frac{(n+1)n^2(n-1)}{2} \ge \frac{kn^2(n-1)}{2}.$$

Hence $n \ge k-1$. The equality takes place if and only if through each point there passes a line, i.e., when the k-net is an affine plane. We have proved:

- If n is the order of a k-net, then $n+1 \ge k$. The equality takes place if and only if the k-net is an affine plane.
- If n the order of a transversal k-design, then $n+1 \ge k$. The equality takes place if and only if the design is the dual of an affine plane.

Projective planes. A projective plane is a system of lines such that there exist four noncollinear points, each two lines intersect in a single point, and each two points are connected by a single line.

The notion of projective plane is self-dual. A removal of a line from a projective plane yields an affine plane. An affine plane may be completed to a projective plane by adding a new point for each pencil of lines. The lines of the pencil meet in this added point (which is called a point 'at infinity'). All points at infinity form a 'line at infinity'.

Building an affine plane. Let $(Q, +, \cdot, 0, 1)$ be an algebra such that (Q, +, 0) is a group, (Q^*, \cdot) is a quasigroup, $Q^* = Q \setminus \{0\}$, and x0 = 0x = 0 for each $x \in Q$. For $a, b \in Q$ put $\ell_{a,b} = \{(\alpha, \beta) \in Q \times Q; \beta = a\alpha + b\}$ and $\ell_{\infty,b} = \{(b, \beta); \beta \in Q\}$. Set $Q_{\infty} = Q \cup \{\infty\}$ and put $\mathcal{L} = \{\ell_{a,b}; (a,b) \in Q_{\infty} \times Q\}$. Elements of \mathcal{L} will be called *lines*. The question when the line systems \mathcal{L} is an affine plane is addressed below. Collineations of \mathcal{L} will be discussed first.

Collineations in the first coordinate. Let us verify that for each $d \in Q$ the mapping $(\alpha, \beta) \to (\alpha, \beta + d)$ is a collineation. This boils down to verifying

$$\ell_{a,b} \to \ell_{a,b+d}$$
 and $\ell_{\infty,b} \to \ell_{\infty,b}$.

However, that is obvious since $\beta = a\alpha + b$ if and only if $\beta + d = a\alpha + (b + d)$.

Collineations in the second coordinate. The mapping $(\alpha, \beta) \rightarrow (\alpha + c, \beta)$ is a collineation for each $c \in Q$ if and only if

$$x(y+z) = xy + xz$$
 for all $x, y, z \in Q$.

Proof. A line $\ell_{\infty,b}$ is mapped upon $\ell_{\infty,b+c}$. A line $\ell_{0,b}$ is mapped upon itself. Let $(a,b) \in Q^* \times Q$. The case c = 0 is trivial, let us have $c \in Q^*$. If $(\alpha,\beta) \to (\alpha+c,\beta)$ is a collineation, then there has to exist $(a',b') \in Q^* \times Q$ such that

$$\beta = a\alpha + b \quad \Leftrightarrow \quad \beta = a'(\alpha + c) + b'.$$

Setting $\alpha = 0$ yields $\beta = b$ and b = a'c + b'. Hence b' = -a'c + b = a'(-c) + b.

Put now $\alpha = -c$. Then a(-c) + b = b' = a'(-c) + b. Therefore a = a', and $a\alpha = a(\alpha + c) - ac$ for all $\alpha \in Q$. The latter equality yields the left distributive law since a and c are assumed to run through Q^* .

Under which conditions does \mathcal{L} induce an affine plane? Fix $a \in Q_{\infty}$ and put $\mathcal{L}_a = \{\ell_{a,b}; b \in Q\}$. Claim: Each point (α, β) belongs to exactly one $\ell \in \mathcal{L}_a$. This is clear if $a = \infty$. Suppose that $a \in Q$, and observe that there exists exactly one $b \in Q$ such that $\beta = a\alpha + b$.

Lines of \mathcal{L}_a thus partition the point set $Q \times Q$. This means that pencils of the purported affine plane have to coincide with sets \mathcal{L}_a .

Let ℓ and ℓ' be lines from different pencils. If $\ell \in \mathcal{L}_{\infty}$ or $\ell \in \mathcal{L}_{0}$, then one of the coordinates is fixed, and that makes ℓ to intersect ℓ' in exactly one point.

Let us have $\ell = \ell_{a,b}$ and $\ell' = \ell_{a',b'}$, where $a, a' \in Q^*$ and $b, b' \in Q$, $a \neq a'$. The lines ℓ and ℓ' intersect in exactly one point if and only if the equation ax + b = a'x + b' has exactly one solution $x \in Q$. Since the equation may be written as a'x = ax + (b - b'), axiom (A2) holds if and only if

$$\forall a, b, c \in Q \colon a \neq b \Rightarrow \exists ! x \in Q \text{ such that } ax + c = bx.$$
 (AF2)

The axiom (A3) holds if any two distinct points (α, β) and (α', β') are contained in exactly one line ℓ . If $\alpha = \alpha'$, then $\ell = \ell_{\infty,\alpha}$. Assume $\alpha \neq \alpha'$. The task is to solve equations $x\alpha + \beta = y = x\alpha' + \beta'$. The solution (x, y) is determined by the value of x uniquely. The equation may be written as $x\alpha + (\beta - \beta') = x\alpha'$. Hence (A3) holds if and only if

$$\forall a, b, c \in Q \colon a \neq b \Rightarrow \exists ! x \in Q \text{ such that } xa + c = xb.$$
 (AF3)

Quasifield defined. Results above bring us to the following definition. A quasifield is an algebra $(Q, +, \cdot, 0, 1)$ such that

- (Q, +, 0) is a group;
- $(Q^*, \cdot, 1)$ is a loop;
- x(y+z) = xy + xz for all $x, y, z \in Q$; and
- for all $a, b, c \in Q$, $a \neq b$ there exists unique $x \in Q$ such that ax = bx + c.

The definition above is the definition of a *left quasifield*. The right quasifield is obtained by using mirror conditions. In the following a *quasifield* means the left quasifield. For the sake of completeness recall that $Q^* = Q \setminus \{0\}$.

Proposition. Let Q be a quasifield. Then a0 = 0a = 0 for every $a \in Q$. Furthermore, a(-b) = -ab and a + b = b + a, for any $a, b \in Q$.

Proof. To prove that a0 = 0 write a0 as a(0+0) = a0 + a0. To prove the mirror equality assume that $0b \neq 0$. Then $b \neq 0$ and there exists $a \in Q^*$ such that ab = 0b. The equation ax = 0x hence possesses two different solutions x = b and x = 0. That is a contradiction.

Note that 0 = a0 = a(b + (-b)) = ab + a(-b) implies a(-b) = -ab, for any $a, b \in Q$.

Suppose now that $a, b \in Q$ are such that $a + b \neq b + a$. This implies $a \neq 0$ and $b \neq 0$. Put t = b + a - b. The assumption is that $t \neq a$. We have $t \neq 0$. There thus exists $s \neq 1$ such that sa = t. Let x be the only solution to x = sx + b. Then

$$x + a - b = sx + b + a - b = sx + t = sx + sa = s(x + a).$$

The equation y - b = sy thus possesses solutions y = x and y = x + a. Hence x = x + a, and a = 0, a contradiction.

Prequasifields. The definition of a prequasifield differs from that of a quasifield by relaxing the assumption of (Q^*, \cdot) being a loop to (Q^*, \cdot) being a quasigroup. Everything above that is true for quasifields remains to be true for prequasifields. This is also the case of the preceding proof since the equation x = sx + b may be replaced by an equation ux = sx + b, where $u \in Q^*$ is chosen in such a way that ua = a.

Prequasifields yield affine planes. Systems $(Q, +, 0, \cdot)$ describe an affine plane with lines $\ell_{a,b}$, $(a,b) \in Q_{\infty} \times Q$, if (Q, +, 0) is a group and both (AF2) and (AF3) hold. This has been proved above. (Conditions (AF2) and (AF3) imply that (Q^*, \cdot) is a quasigroup, as may be verified easily.) To see that a prequasifield can be used to construct an affine plane note that (AF2) is one of its axioms, while (AF3) follows from the left distributivity since xa = xb + c may be written as x(a - b) = c.

Left division and the left distributive law. Suppose that (Q, +, 0) is a group and that \cdot is a binary operation upon Q such that (Q^*, \cdot) a quasigroup. If \cdot and + are connected by the left distributive law, then the equation a(0 + 0) = a0 + a0implies a0 = 0 like above. Set $a \setminus 0 = 0$, for each $a \in Q$.

The equality a(b+c) = ab+ac holds for all $b, c \in Q$ if and only if $L_a \in \text{End}(Q, +)$. If $a \in Q^*$, then in fact this is the same as $L_a \in \text{Aut}(Q, +)$, and thus also the same as $L_a^{-1} \in \text{Aut}(Q, +)$. Since $L_a^{-1}(b) = a \setminus b$ we can state that

 $(\forall x,y,z\in Q \ x(y+z)=xy+xz) \ \Rightarrow \ (\forall x,y,z\in Q \ x\backslash(y+z)=x\backslash y+x\backslash z).$

Principal loop isotopes of a prequasifield. Let e and f be nonzero elements of a prequasifield $(Q, +, \cdot, 0)$. If $x * y = (x/f)(e \setminus y)$ for all $x, y \in Q$, then (Q, +, *, 0, ef) is a quasifield.

Proof. If $a, b, c \in Q$, then

 $\begin{aligned} a*(b+c) &= a/f \cdot e \setminus (b+c) = a/f \cdot (e \setminus b + e \setminus c) = (a/f)(e \setminus b) + (a/f)(e \setminus c) = a*b + a*c. \\ \text{A solution to } a*x &= b*x + c, \ a \neq b, \text{ has to fulfil } a/f \cdot e \setminus x = b/f \cdot e \setminus x + c. \\ \text{This determines } x \text{ uniquely since } e \setminus x = d, \text{ where } d \text{ is the only solution to } a/f \cdot y = b/f \cdot y + c. \end{aligned}$

Collineation induced by isotopy. The mapping $(\alpha, \beta) \mapsto (e\alpha, \beta)$ yields a collineation of the affine plane induced by a prequasifield $(Q, +, \cdot, 0)$ on the affine plane induced by the quasifield (Q, +, *, 0, ef), where $e, f \in Q^*$ and $x * y = x/f \cdot e \setminus y$ for all $x, y \in Q$.

Proof. Lines $\ell_{a,b}$ are given by solutions to y = ax + b. Lines $\ell_{a,b}^*$ are given by solutions to y = a * x + b. We have $(\alpha, \beta) \in \ell_{a,b}$ if and only if $\beta = (af) * (e\alpha) + b$, i.e., if and only if $(e\alpha, \beta) \in \ell_{af,b}^*$.

Furthermore, the line $\ell_{\infty,b}$ is mapped upon $\ell_{\infty,eb}^*$ since $\alpha = b$ if and only if $e\alpha = eb$.

Finite quasifields. Let (Q, +, 0) be a group and $(Q^*, *)$ a quasigroup that are connected by the left distributive law. Then a0 = 0 and a(-b) = -ab, for all $a, b \in Q$. However there is no way how to prove 0a = 0. To see this suppose that the latter holds and change it to $0a = \varphi(a)$, where $\varphi \in \text{End}(Q, +)$. That does not change the assumptions on + and \cdot .

However, if 0a = 0 for all $a \in Q$, then there exists at most one $x \in Q$ such that ax = bx+c, whenever $a, b, c \in Q$ and $a \neq b$. To see this assume that ax = bx+c and ay = by+c. Then -bx + ax = -by + ay, ax - ay = bx - by and a(x-y) = b(x-y). This is not possible if $x - y \neq 0$.

By the same token there cannot be -bx + ax - c = -by + ay - c if $a, b, c, x, y \in Q$, $a \neq b$ and $x \neq y$. The mapping $x \mapsto -bx + ax - c$ is hence an injective mapping $Q \to Q$ whenever $a, b, c \in Q$ and $a \neq b$. If Q is finite, then there exists $x \in Q$ such that -bx + ax - c = 0, which means ax = bx + c. This shows that in the finite case a prequasifield may be defined by assuming that (Q, +, 0) is a group, (Q^*, \cdot) a quasigroup, 0a = 0 for all $a \in Q$, and a(b + c) = ab + ac for all $a, b, c \in Q$.

Furthermore, verifying that (Q^*, \cdot) is a quasigroup may be simplified if

$$ab = 0 \iff a = 0 \text{ or } b = 0, \text{ for all } a, b \in Q.$$
 (Z)

If the latter holds, then each L_a , $a \in Q^*$, has to be injective (and thus bijective in the finite case) since ax = ay if and only if a(x - y) = 0.

Semifields. A semifield $(S, +, \cdot, 0, 1)$ is an algebra such that (S, +, 0) is a group, $(S^*, \cdot, 1)$ is a loop, and both distributive laws hold (thus a(b + c) = ab + ac and (b + c)a = ba + ca for all $a, b, c \in S$.) A presemifield does not require the existence of the unit element.

By standard arguments, a0 = 0 = 0a and a(-b) = -ab = (-a)b, for all $a, b \in S$. Each semifield is a quasifield since if ax = bx + c and $a \neq b$, then -bx + ax = (-b + a)x = c, and that determines x uniquely. For the finite (pre)semifield the quasigroup property of \cdot may be replaced by (Z).

Note that the definition of a semifield differs from the definition of a division ring (a skewfield) by dropping the associativity of the multiplication.

Nearfields. A *nearfield* $(N, +, \cdot, 0, 1)$ is an algebra such that both (N, +, 0) and $(N^*, \cdot, 1)$ are groups, and the left distributive law holds.

By standard arguments, a0 = 0 and a(-b) = -ab for all $a, b \in N$. If $0b \neq 0$, then a(0b) = (a0)b = 0b for all $a \in N$. That cannot be true if N^* is nontrivial, i.e. if $|N| \ge 3$. On two elements the definition above allows for the multiplication given by xy = y. This is an exceptional case that is not regarded to be a nearfield. To avoid it, the axioms may be extended by stating explicitly that 0x = 0 for all $x \in N$.

A finite nearfield fulfils the conditions of finite quasifield. An infinite nearfield need not be a quasifield. However, it may be proved that every nearfield N fulfils a + b = b + a and (-a)b = -ab, for all $a, b \in N$. A nearfield which is a quasifield is called *planar* as it determines an affine plane (and thus also a projective plane).

Note that the definition of a nearfield differs from the definition of a division ring (a skewfield) by dropping the right distributive law. In fact, our definition is that of the *left nearfield*. The *right nearfield* assumes the right distributive law.

Connections to projective planes. If a is a point and ℓ a line of a projective plane then there may exist a collineation called *perspectivity* that is determined uniquely by (a, ℓ) (a is called the center and ℓ the axis). Projective planes determined by division rings contain a perspectivity for each pair (a, ℓ) . In fact this a way how to characterize them. Assumptions of the form that a perspectivity exists for certain pairs (a, ℓ) gives rise to notions of quasifield, semifield, nearfield in the sense that if the respective assumptions are fulfilled, then the projective plane induces an affine plane that may be coordinatized by a quasifield or a semifield or a nearfield.

Remarks on coordinatization and isotopy. Note that above we have proved that affine planes coordinatized by isotopic prequasifields are isomorphic. From the geometric standpoint isotopic quasifields are nothing else but different coordinatizations of the same geometric structure.

Note that a principal isotope $x/f \cdot e \setminus y$ of a semifield is again a semifield, and that the same is true for nearfields. Two semifields (or nearfields) are said to be isotopic, if one of them is isomorphic to the principal isotope of the other. It is easy to adapt Albert's theorem to nearfields, showing thus that isotopic nearfields are isomorphic.