MATH. SCAND. 5 (1957), 197–201

# ON THE RELATION OF CONGRUENCE IN FINITE GEOMETRIES

PAUL KUSTAANHEIMO

It is a well-known fact that the incidence axioms I: 1–8, IV of Hilbert [2] or the corresponding axioms for a Euclidean incidence geometry of $n$ dimensions can be satisfied by finite models, i.e. by models containing only a finite number of points, lines, planes etc., these models being the linear vector spaces of $n$ dimensions over finite fields $GF_q$, $q=p^h$. Any two natural numbers $n$ and $h$ and any prime $p$ give one and to within isomorphism only one such geometry.

The question whether the axioms of order and the axioms of congruence are also satisfiable in finite geometries has been proposed much later, chiefly by G. Järnefelt (cf. [3] and [6]) in connection with the problem of a finite physics (cf. [4] and [5]).

As to the relation of order in finite geometries, the problem was solved by E. Sperner [13] [14] and by the author [7] in two somewhat different ways for the case $p \neq 2$, and recently by the author [8] also for the case $p=2$.

As to the relation of congruence in finite geometries, the problem was partially solved in Järnefelt–Kustaanheimo [6], but only in those cases where $p \neq 2$, $h=1$, $n=2$. In this paper the solution will be given for the cases $p \neq 2$, $n=2$, $h$ arbitrary. In all other cases, that is, $p=2$ or $n>2$, the problem is still open.

Two important theorems having been demonstrated by B. Segre [10] [11] and P. Bernays [1], it is now possible to show in a somewhat simplified way that the five axioms III.0–4, given in Järnefelt–Kustaanheimo [6], define a unique relation of congruence in the finite Euclidean plane over any Galois field $GF_q$, $q=p^h$, $p \neq 2$.

The axiom III.2 in Järnefelt–Kustaanheimo [6] is not sufficient in the general case $h \neq 1$ and must be replaced by the axiom 3 in this paper, both axioms being equivalent in the case $h=1$. The other axioms remain essentially the same, and all the five axioms are repeated here.

Received July 3, 1957.

We write shortly "$AB=CD$" for the proposition "the segment between the points $A$ and $B$ is congruent with the segment between the points $C$ and $D$".

AXIOM 1. $AB=CD$ implies $BA=CD$ and $CD=AB$. $AB=CD$ and $CD=EF$ imply $AB=EF$.

AXIOM 2. If $AB$ and $CD$ are parallel, then $AB=CD$ is valid when and only when either $AC$ is parallel to $BD$ or $AD$ is parallel to $BC$.

AXIOM 3. If $A$, $B$, $C$, $D$ are four collinear points and $A'$, $B'$, $C'$, $D'$ are four collinear points, and the lines $AA'$, $BB'$, $CC'$, $DD'$ are parallel, then $AB=A'B'$ implies $CD=C'D'$.

AXIOM 4. If $A$, $B$, $C$ are three distinct collinear points and $A'$, $B'$, $C'$ are collinear, then $AB=A'B'$, $AC=A'C'$, $BC=B'C'$, $AD=A'D'$, and $BD=B'D'$ imply $CD=C'D'$.

AXIOM 5. There exist four points $A$, $B$, $C$, $D$ such that for any two points $E$, $F$ there exists a point $G$ such that $E$, $F$, $G$ are collinear and either $AB=EG$ or $CD=EG$.

Axiom 2 gives immediately the following two theorems.

THEOREM 1. *$AA=BC$ implies $B=C$.*

THEOREM 2. *If $A$, $B$ are two distinct points, then there exists one and only one point $C$ such that $A$, $B$, $C$ are collinear, $B\neq C$, and $AB=AC$.*

Theorem 2 is demonstrated by constructing a parallelogram $ABDE$. According to axiom 2, $AB=AC$ is valid when and only when $CADE$ is a parallelogram, too. From this construction follows also that the coordinates of $A$ equal the mean values of the corresponding coordinates of $B$ and $C$.

Axiom 3 gives the following theorem or corollary.

THEOREM 3. *If $O$, $I$, $K$ are three distinct collinear points, $O$, $J$, $L$ are three distinct collinear points, and $IJ$ is parallel to $KL$, then $OI=OJ$ implies $OK=OL$.*

In order to decide whether or not a given proposition $EF=GH$ is valid, we may use the transitivity stated by axiom 1 and replace the segments $EF$ and $GH$ by other segments, e.g. by two segments $OI$ and $OJ$, where $O$ is any chosen point and $OE$ parallel to $IF$, $OI$ parallel to $EF$, $OG$ parallel to $JH$, and $OJ$ parallel to $GH$. According to axiom 2, the proposition $OI=OJ$ is now equivalent to $EF=GH$. According to axiom 3, we can further shorten or lengthen the segments $OI$ and $OJ$, by the construction mentioned in theorem 3, so that one of them attains some given standard length.

Thus the relation of congruence is decidable if we can construct two sets of points, $X$ and $Y$, such that $OX = AB$ for all $X$, and $OY = CD$ for all $Y$, where $A$, $B$, $C$, $D$ are e.g. those four points $A$, $B$, $C$, $D$ assumed to exist by axiom 5. We call these two point sets the measure curves.

Let the set of all points $X$ satisfying $OX = AB$ be one of the measure curves. According to theorem 2, every line passing through $O$ meets the measure curve in either exactly two or exactly no points. Now we shall demonstrate that also every line not passing through $O$ meets the measure curve in at most two points.

Let us suppose that a line $EFG$ not passing through $O$ meets the measure curve in at least three distinct points $E$, $F$, $G$. We choose a point $H$ so that $O \neq H$ and $OH$ parallel to $EFG$. We draw through $H$ a line parallel to $OG$. Let $I$ be that point where this line meets the line $OE$, and $J$ that point where this line meets the line $OF$. Let $K$ and $L$ be points on the line $OG$ such that $IK$ and $JL$ are parallel to $OH$. According to axiom 2, we now have $HI = OK$, $IJ = KL$, $HJ = OL$, and according to theorem 3, $OI = OK$, $OJ = OL$. Thus, according to axiom 4, we have also $OH = OO$. But this is a contradiction, according to theorem 1.

Thus every line meets the measure curve in at most two points, or, using a term introduced by Segre [12], the measure curve is a $k$-arc. It is a well known fact (cf. Segre [12] and Qvist [9]) that a $k$-arc contains at most $q+1$ points when $p \neq 2$. On the other hand, both measure curves together must contain at least $2(q+1)$ points, according to axiom 5 and theorem 2. Thus we conclude that each measure curve contains exactly $q+1$ points, i.e. each measure curve is a $(q+1)$-arc or an oval, using another term introduced by Segre [10] [11].

Segre [10] [11] has demonstrated that every oval is an ellipse. Using a coordinate system $x$, $y$ with $O$ as origo, the measure curves can thus be represented by two equations

$$x^2 + a'xy + b'y^2 = g\,, \tag{1}$$

$$x^2 + cxy + dy^2 = h \tag{2}$$

where $a'^2 - 4b'$ and $c^2 - 4d$ are non-squares in $GF_q$. Linear terms in $x$ and $y$ are lacking because of the symmetry stated by theorem 2.

Using a linear coordinate transformation, we may transform the left-hand side of (2) in some given standard form, e.g. $x^2 - ky^2$, where $k$ is any given non-square of $GF_q$ (cf. Järnefelt–Kustaanheimo [6]). In this new coordinate system the equations (1) and (2) read

$$x^2+axy+by^2 = g\,, \tag{3}$$

$$x^2-ky^2 = h\,, \tag{4}$$

where $a^2-4b$ is a non-square.

According to axiom 5, every line through $O$ must meet at least one of the measure curves, and then in exactly two points, according to theorem 2. The total number of points on both measure curves being $2(q+1)$, we conclude that no line through $O$ meets both measure curves. A theorem, demonstrated by Bernays [1], states that this is possible only if $a=0$ and $b=-k$. We reproduce here the proof of Bernays.

Let us consider the $x$-axis which is a line through $O$. It must meet exactly one of the curves (3) and (4). Thus one of the numbers $g$ and $h$ is a square and the other a non-square, e.g. $g$ a square and $h$ a non-square. Now let us consider the line passing through $O$ and a point $(x, y)$. It meets (3) when and only when $x^2+axy+by^2$ is a square, and it meets (4) when and only when $x^2-ky^2$ is a non-square. In order that the line meet one and only one of the curves (3) and (4), it is thus necessary and sufficient that

$$\frac{x^2+axy+by^2}{x^2-ky^2} \tag{5}$$

be a square for all values $x$, $y$. We consider only values $y=1$ and $x$ running through all the $q$ elements of $GF_q$. The expression (5) being always $\neq 0$, it can assume only $\frac{1}{2}(q-1)$ different values. Thus there exist three different values $x_1$, $x_2$, $x_3$, satisfying

$$\frac{x_1^2+ax_1+b}{x_1^2-k} = \frac{x_2^2+ax_2+b}{x_2^2-k} = \frac{x_3^2+ax_3+b}{x_3^2-k}$$

or

$$ax_1+b+k = ax_2+b+k = ax_3+b+k = 0\,.$$

But this is possible only if $a=b+k=0$. Thus, instead of (3) and (4) we can write

$$x^2-ky^2 = g\,, \tag{6}$$

$$x^2-ky^2 = h\,. \tag{7}$$

Finally, according to axioms 3 and 5, we may use some other standards of length, $AB$ and $CD$, and thus transform the right-hand sides of (6) and (7) e.g. into 1 and $k$, where $k$ is the same given non-square as on the left-hand side. Instead of (6) and (7) we then have

$$x^2-ky^2 = 1\,, \tag{8}$$

$$x^2-ky^2 = k\,, \tag{9}$$

where the last remaining parameter $k$ can be fixed to be any given non-square.

The five axioms 1–5 determine thus the relation of congruence uniquely to within an isomorphic mapping leaving the relations of incidence and congruence invariant.

## REFERENCES


1. P. Bernays, Letter to the author, dated May 11, 1952, Zürich.
2. D. Hilbert, *Grundlagen der Geometrie*, 8. Aufl., Leipzig, 1956.
3. G. Järnefelt, *A plane geometry with a finite number of elements*, Veröffentlichungen Finn. Geodät. Inst. 36 (1949), 71–80.
4. G. Järnefelt, *Ein endliches Weltbild*, Vortrag gehalten am 9. Oktober 1953 in der Finnischen Akademie der Wissenschaften, Sonderdruck des Astronomischen Observatoriums in Helsinki.
5. G. Järnefelt, *On a finite approximation to the energy spectrum of the linear harmonic oscillator*, 13$^{e}$ congr. mathém. scand. Helsinki 1957.
6. G. Järnefelt and P. Kustaanheimo, *An observation on finite geometries*, C. R. 11$^{e}$ congr. mathém. scand. Trondheim 1949, 166–182.
7. P. Kustaanheimo, *A note on a finite approximation of the Euclidean plane geometry*, Soc. Sci. Fenn. Comment. Phys-Math. 15, no. 19 (1950), 11 pp.
8. P. Kustaanheimo, *On the relation of order in finite geometries*, 13$^{e}$ congr. mathém. scand. Helsinki 1957.
9. B. Qvist, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fennicae, Ser. A, I Math.-Phys. no. 134 (1952), 27 pp.
10. B. Segre, *Sulle ovali nei piani lineari finiti*, Rend. Accad. Naz. Lincei (8) 17 (1954), 141–142.
11. B. Segre, *Ovals in a finite projective plane*, Canadian J. Math. 7 (1955), 414–416.
12. B. Segre, *Curve razionali normali e k-archi negli spazi finiti*, Ann. Mat. Pura Appl. (4) 39 (1955), 357–379.
13. E. Sperner, *Die Ordnungsfunktionen einer Geometrie*, Math. Ann. 121 (1949), 107–130.
14. E. Sperner, *Beziehungen zwischen geometrischer und algebraischer Anordnung*, S.-B. Heidelberger Akad. Wiss. Math. Nat. Kl. 1949, 413–448.


ASTRONOMICAL OBSERVATORY, HELSINKI, FINLAND