Riemann's formula (6.3). The Lebesgue sums use a "horizontal" division of the y-values, while the Riemann sums have a "vertical" division of the x-axis.

The following characterisation of the Riemann integrable functions will throw a final light on our subject: A function $f(x)$ is integrable in the Riemann sense if, and only if, it is measurable and bounded in $\langle a, b \rangle$, and if the set of its points of discontinuity has the linear Lebesgue measure zero.

KING'S COLLEGE,
NEWCASTLE-ON-TYNE.

Finite projective geometry.

By A. G. WALKER.

1. The following description of the projective geometry of a finite number of points in 2-space is almost certainly known to those acquainted with projective geometry or with modern algebra. The object of this brief account is to show how certain finite systems can be presented in a form easily understood by students, and how they provide simple but instructive examples of fundamental ideas and "constructions." The fact that these examples belong to a geometry which is essentially non-Euclidean has great teaching value to those students who are apt to confuse projective geometry with the "method of projection" in Euclidean geometry. The underlying algebra is described briefly in § 4, but an understanding of this is not essential to the geometry. This algebraic work may, however, be of interest to those to whom Galois fields are fairly new.

2. The axioms generally adopted for projective geometry of 2-space are nine in number, being the three axioms of incidence (there is one and only one line passing through two points, and two lines have a point in common), the three axioms of extension (there is at least one line and at least three points on every line, and not all points lie on the same line), the axiom of perspective triangles (Desargues' theorem), the projective axiom (Pappus' theorem), and the diagonal axiom (the three diagonal points of a quadrangle are not

https://doi.org/10.1017/S0950184300002731 Published online by Cambridge University Press

collinear). These axioms are found to be sufficient to give those properties of points, lines, conics, etc., which are familiar as projective invariants of Euclidean geometry. Euclidean geometry (with infinity) is not, however, the only system satisfying the above axioms, and there are others which are particularly interesting in that each consists of only a finite number of points. A well known example is the system of 13 points and 13 lines with four points on each; denoting the points by 0, 1, 2, ..., 12, then the linear sets of points are the columns in the following array:

0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
3	4	5	6	7	8	9	10	11	12	0	1	2
9	10	11	12	0	1	2	3	4	5	6	7	8.

It can be verified that all nine axioms are satisfied by this system.

The problem of finding the most general finite system which satisfies the projective axioms is algebraic, but the results can always be expressed in a non-algebraic form as in the case of the above 13-point system. A system of this kind exists for every pair of positive integers p, m, where p is a prime number ($p > 2$). Writing $n = p^m$ and $N = n(n+1)$, then there are in this system $N+1$ points and $N+1$ lines, with $n+1$ points on every line and $n+1$ lines through every point. There are also $n^2(n^3-1)$ conics, and $n+1$ points on every conic. For a given conic, $\frac{1}{2}n(n+1)$ lines are chords, $n+1$ lines are tangents (*i.e.* meet the conic only once), and the remaining $\frac{1}{2}n(n-1)$ lines do not meet the conic. Every point has a polar, but this line need not meet the conic, *i.e.* the polar is not always the chord of contact of tangents. All these results and many others can be deduced immediately from the axioms and the fact that there are exactly $n+1$ points on at least one line.

It is an interesting fact that the $N+1$ points of the general finite system can be denoted by 0, 1, 2, ..., N in such a way that the $N+1$ lines are the columns of a cyclic array, as in the case of the 13-point system described above ($n = 3$). For such an arrangement, all that need be known is the first column, and the remaining N columns are then obtained by cyclic progression. This first column will be called the *key* of the system, thus the key of the 13-point system is 0, 1, 3, 9.

In the following table are keys calculated for a number of systems, the case $p = 2$ (in which the diagonal axiom is denied) being included for algebraic interest. Their calculation, and the meaning of the third column, will be explained later.

n	N	Generating cubic	Key
2	6	$x^3 - x - 1$	0, 1, 3
3	12	$x^3 - x - 1$	0, 1, 3, 9
2^2	20	$x^3 - x^2 - x - i\ (i^2 = i + 1)$	0, 1, 4, 14, 16
5	30	$x^3 + x - 1$	0, 1, 3, 8, 12, 18
7	56	$x^3 - x - 2$	0, 1, 3, 13, 32, 36, 43, 52
2^3	72	$x^3 - jx - 1\ (j^3 = j + 1)$	0, 1, 3, 7, 15, 31, 36, 54, 63
3^2	90	$x^3 - kx - 1\ (k^2 = 2)$	0, 1, 3, 9, 27, 49, 56, 61, 77, 81
11	132	$x^3 + 4x - 1$	0, 1, 3, 15, 46, 71, 75, 84, 94, 101. 112, 128,

3. A convenient system which is useful for demonstration purposes is that given by $n = 5$, the complete cyclic array being

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11
18	19	20	21	22	23	24	25	26	27	28	29	30	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

The line whose column is headed by r will be denoted by $\bar{r}$, and we shall write $r.s$ for the line joining points r and s, $\bar{r}.\bar{s}$ for the point of intersection of lines $\bar{r}$ and $\bar{s}$, and $r.s:u.v$ for the point of intersection of lines $r.s$ and $u.v$. A few simple examples of suitable problems in this particular system are as follows.

(i.) On the line $\bar{0}$, find the harmonic conjugate of 0 with respect to 12 and 18.

The usual quadrangular construction is as follows. Take two points collinear with 0, say 2 and 7 on line $\overline{30}$. Then from the array we find

$$2.12:7.18 = \overline{25}.\bar{6} = 6, \qquad 2.18:7.12 = \overline{15}.\bar{4} = 16.$$

The required point is therefore the intersection of $\bar{0}$ and 6.16, *i.e.* is $\bar{0}.\overline{29} = 1$.

(ii.) Prove that the points 5, 10, 12, 18, 24, 29 lie on a conic.

Testing by Pascal's theorem, the meets of opposite sides of this hexagon are found to be

$$5.10:18.24 = \bar{2}.\bar{6} = 14,\ 10.12:24.29 = \bar{9}.\overline{21} = 21,\ 12.18:29.5 = \bar{0}.\overline{28} = 0.$$

The three points 14, 21, 0 are collinear ($\overline{13}$) as required.

(iii.) Find the tangent at the point 5 of the conic of (ii).

The simplest method is to note that of all the lines through 5, $\overline{5}$ is the only one which does not meet the conic again; $\overline{5}$ is therefore the tangent. Another method is to apply Pascal's theorem to the hexagon 5, 5, 10, 12, 18, 24.

(iv.) Find the polar of the point 2 with respect to the conic of (ii).

Examining the lines through 2, we see that two of them, $\overline{15}$ and $\overline{25}$, each meet the conic just once, at 18 and 12 respectively. These lines are therefore tangents, and the polar of 2 is the chord of contact, *i.e.* the line $18.12 = \overline{0}$. Another method is described in (v).

(v.) Find the polar of 0 with respect to the conic of (ii).

In this case we find that there are no tangents from the point to the conic, and our method now is to use the harmonic properties of an inscribed quadrangle. Two chords through 0 are $\overline{0}$ and $\overline{23}$, meeting the conic at 12, 18 and 10, 24 respectively. The polar of 0 is the line joining the other two diagonal points of the quadrangle formed by these four points, and we find

$$12.10:18.24 = \overline{9}.\overline{6} = 9, \qquad 12.24:18.10 = \overline{12}.\overline{10} = 13, \qquad 9.13 = \overline{1}.$$

Hence $\overline{1}$ is the required line. It may be noted that this line passes through the point found in ex. (i), as would be expected.

These are only a few of the many elementary but instructive exercises which can be set in this particular system of geometry.

4. The algebra associated with a finite system of projective geometry is that of a Galois field, G. The order, or number of elements, is of the form $n = p^m$ where p is prime, and there are p "integers," which can be written[1] $0, 1, 2, \ldots, p-1$. A point is now defined as (x, y, z) where x, y, z belong to G and are not all zero, and (kx, ky, kz) is the same point for all $k \neq 0$. A line is defined as $\{a, b, c\}$, where a, b, c belong to G and are not all zero, and is the class of points satisfying $ax + by + cz = 0$. It now follows that the first eight projective axioms are satisfied, and that the diagonal axiom is satisfied provided $p > 2$. Also, there are $n + 1$ points on every line,

[1] An algebraic combination of these integers in G is the numerical residue mod. p. Thus when $p = 5$, we have $2 + 2 = 4$, $3 + 4 = 2$, $2 \times 4 = 3$, $1/3 = 2$ et

https://doi.org/10.1017/S0950184300002731 Published online by Cambridge University Press

etc., and we therefore have an algebraic representation of the general finite system described earlier.

We shall now show how a cyclic array as described in § 2 can be determined for any finite system. Consider a cubic $C = x^3 - ax^2 - bx - c$, where a, b, c belong to G and are such that C is irreducible, *i.e.* $C = 0$ has no root in G. Then it can be proved that C divides $x^{N+1} - c$, where $N = n(n+1)$ as before. It is also possible that C divides $x^M - d$ for some d of G and some $M < N + 1$; if no such M exists, we shall say that C is *primitive*. When $n = 7$, for example, we find that $x^3 - x - 1$ is reducible, being $(x + 2) \times (x^2 - 2x + 3)$, that $x^3 - 3x - 1$ is irreducible but not primitive since it divides $x^{19} + 3$, and that $x^3 - x - 2$ is primitive. It is easily verified that when $N + 1$ is prime, then every irreducible cubic is primitive.

Suppose now that the above cubic is primitive, and consider the sequence u_r of elements in G defined by

$$u_0 = 0,\ u_1 = 0,\ u_2 = 1,\ u_{r+3} = au_{r+2} + bu_{r+1} + cu_r \quad (r = 0, 1, 2, \ldots.).$$

Then it can be proved that $u_{N+s} = cu_{s-1}$ $(s = 1, 2, \ldots.)$, and that no relation of this form holds (for all s) with c replaced by any element of G and N replaced by a lesser number. The sequence is thus periodic with period $N + 1$ except for the multiplier c which enters at each new period. If now a point r is defined as (u_r, u_{r+1}, u_{r+2}) for each r, then we get distinct points for $r = 0, 1, 2, \ldots., N$, after which there is cyclic repetition. These $N + 1$ points are therefore all the points of the 2-space under consideration, and they have the desired cyclic symmetry in the order in which they arise. The lines are given by the columns in the array of which the key consists of the successive values of r for which $u_r = 0$ (this key being the line $x = 0$).

There are different primitive cubics for the same Galois field, and these generate different cyclic arrays for the same geometrical system. Except in the case $n = 2^2$ we can always choose $a = 0$, so that the key starts with 0, 1, 3. We also take $c = 1$ whenever possible, for then the sequence u_r is truly periodic. The primitive cubics which generate the keys given in § 2 are seen in the third column of the table. As an example of an alternative, there is also for $n = 5$ the key 0, 1, 3, 10, 14, 26, which is generated by $x^3 - 3x - 1$.

As an illustration of the general method, consider $n = 5$, and take the primitive cubic $x^3 + x - 1$ given in the table. Then the sequence u_r is found to be

https://doi.org/10.1017/S0950184300002731 Published online by Cambridge University Press

0	5	10	15	20	25	30
00104	11303	32012	44301	34341	43211	1,0010.....

As expected, the sequence recurs after 31 terms. The coordinates of the point r are now (u_r, u_{r+1}, u_{r+2}) taken from this sequence; thus the point 25 is (4, 3, 2) or a set of elements proportional to these, such as $(1, 2, 3) = 4\,(4, 3, 2)$. The line $\bar{r}$ joins the points r and $r+1$, and it can be verified that this line is $\{v_{r+2}, v_r, v_{r+1}\}$ where

$$v_0 = 0,\ v_1 = 0,\ v_2 = 1,\ v_{r+3} = v_{r+2} + v_r \quad (r = 0, 1, 2, \ldots.).$$

The sequence v_r is

0	5	10	15	20	25	30
00111	23414	34310	34421	02330	31140	1,0011....

and recurs after 31 terms.

The problems solved from the array in § 3 can now be worked algebraically. It can be verified, for example, that the six points in (ii) lie on the conic $4x^2 + y^2 + z^2 + 2zx = 0$. The point 5 is (1, 1, 3) and by the usual formula the tangent at this point is $\{2, 1, 4\} \propto \{4, 2, 3\}$ which is line $\bar{5}$, as found in (iii). The point 2 is (1, 0, 4), and its polar is $\{3, 0, 0\} \propto \{1, 0, 0\}$ which is line $\bar{0}$, as found in (iv). And so on, for other examples.

5. In conclusion it may be mentioned that the extension of these results to spaces of higher dimensions is obvious. In 3-space, for example, there are $n^3 + n^2 + n + 1$ points and the same number of planes, with $n^2 + n + 1$ points on each plane and $n + 1$ points on each line; here n is of the form p^m as before. Algebraically, the points in 3-space are given by $(u_r, u_{r+1}, u_{r+2}, u_{r+3})$, $r = 0, 1, 2, \ldots, n^3 + n^2 + n$, where $u_0 = u_1 = u_2 = 0$, $u_3 = 1$, and u_r is generated by means of a primitive quartic in the Galois field. The system can be described by a cyclic array of $n^2 + n + 1$ rows and $n^3 + n^2 + n + 1$ columns, the points in each column being coplanar. For example, with $n = 2$, writing $0, 1, \ldots, 14$ for the 15 points of 3-space, then the array giving the 15 planes has in the first column 0, 1, 2, 4, 5, 8, 10, and the other columns are found by cyclic progression. In this example the primitive quartic is $x^4 - x - 1$.

DEPARTMENT OF PURE MATHEMATICS,
UNIVERSITY OF LIVERPOOL.