LECTURES ON PROJECTIVE PLANES

RALPH FREESE

A *projective plane* can be formally axiomatized as a triple $\langle \mathcal{P}, \mathcal{L}, I \rangle$, where $\mathcal{P}$ is the set of *points*, $\mathcal{L}$ is the set of *lines*, and $I \subseteq \mathcal{P} \times \mathcal{L}$ is an incidence relation between them satisfying the axions:

(1) Each pair of distinct points determines a unique line.
(2) Each pair of distinct lines determines a unique point.
(3) There is a *quadrangle*, i.e., four points, no three on a line.

(Note we use the obvious geometric and combinatorial terminology.)

Here are some factoids:

- If we take I as an order relation and add a least and greatest element we obtain a modular lattice of height 3.
- The dual of a projective plane is also a projective plane (but not always isomorphic to the original plane).
- The number of points on a line is invariant; the *order* of a plane is one less than this number.

Coordinates. Take a quadrangle O, E, X, and Y. Let R be a set of size n, where n is the order of the plane. Give the points and lines of the plane coordinates as indicated in the figures. Define a ternary operation on R by

$$y = t(x, m, k) \qquad \text{if and only if} \qquad [x, y] \; I \; \langle m, k \rangle.$$

For a plane coordinatized by a (skew) field this just says that $y = xm + k$. The algebra $\mathbf{R} = \langle R, t, 0, 1 \rangle$ so constructed satisfies:

(1) $t(0, a, b) = t(a, 0, b) = b$.
(2) $t(1, a, 0) = t(a, 1, 0) = a$.
(3) Given a, b, c, and d with $a \neq c$, there is a unique x such that $t(x, a, b) = t(x, c, d)$.
(4) Given a, b, c there is a unique x such that $t(a, b, x) = c$.
(5) Given a, b, c, and d with $a \neq c$, there is a unique pair x, y such that $t(a, x, y) = b$ and $t(c, x, y) = d$.

A finite algebra satisfying the first, second and fourth condition will satisfy the third if and only if it satisfies the fifth. A algebra satisfying these axioms is called a *planar ternary ring*. The Germans use the more appropriate term *ternary field*. Any ternary field can be used to coordinatize a projective plane.

Date: June 12, 1996, slightly revised April 4, 1997, and again October 17, 2015.
This research was partially supported by NSF grant no. DMS–9500752.

Although there has been a great deal of work on projective planes, there is not much on ternary fields. One wonders if tame congruence theory, especially some of the extensions mentioned in Keith's talk, might help. Here is an unpublished result of mine:

Theorem 1. *A finite ternary field has a ternary discriminator.*

If $\mathbf{R}$ is a ternary field then the term operations

$$x + y = t(1, x, y)$$
$$x \circ y = t(x, y, 0)$$

are both loops with identity elements 0 and 1, respectively. Not all ternary fields satisfy $t(a, b, c) = a \circ b + c$; those that do are called *linear*. In such ternary rings we will often take $\circ$ and $+$ as the basic operations.

Homogeneous Coordinates. The lattice of subspaces of a three dimension vector space over a skewfield $\mathbf{F}$ forms a projective plane. The points are the one dimensional subspaces and so can be represented by any nonzero member. To make a 'normal form' we pick any nonzero member, and multiply the vector by the reciprocal of the third coordinate if this is not zero. Otherwise we use the first coordinate unless that is also 0. If both are 0 we use $[0, 1, 0]$. Thus the points are the vectors

$[-x, y, 1]$	ordinary affine point (x, y)
$[1, -m, 0]$	point at infinity on all lines of slope m
$[0, 1, 0]$	end of the y–axis

Similarly we represent the lines with the vectors:

$\langle m, 1, -b\rangle$	line of slope m and y–intercept b
$\langle 1, 0, a\rangle$	vertical line through $(a, 0)$
$\langle 0, 0, 1\rangle$	line at infinity

With this setup a point is incident with a line if and only if their dot product is 0. In fact, if $\mathbf{R}$ is a linear ternary field such that $\langle R, +\rangle$ is a group and $(-a)b = -ab$, then the plane coordinatized in this way will be isomorphic to the one coordinatized by the ternary field (in the usual way).

Hall Planes

A *right quasifield* is a linear ternary field in which $+$ is associative (Cartesian group) and the right distributive law holds: $(a + b)c = ac + bc$.

Lemma 2. *Addition is commutative in a right quasifield and* $(-a)b = -ab$.

Proof: For the second $0 = (-a + a)b = (-a)b + ab$, showing $(-a)b = -ab$. The commutativity is harder, but we don't need it.

Let **F** be a field and let

$$f(x) = x^2 - rx - s$$

be an irreducible polynomial over **F**. Let $R = F \times F$. Define addition on R coordinatewise and multiplication by

$$(a,b) \circ (c,d) = \begin{cases} (ac, bc) & \text{if } d = 0 \\ (ac - bd^{-1}f(c), ad - bc + br) & \text{if } d \neq 0 \end{cases} \tag{1}$$

Then $\mathbf{R} = \langle R, +, \circ, 0, 1\rangle$ is a right quasifield known as a *Hall quasifield*. **F** can be viewed as a subalgebra under the embedding $a \mapsto (a, 0)$. These elements commute with all elements of **R**. Moreover, if $a \in F$ then $a(xy) = (ax)y$. Easy calculations prove the next lemma which incidently shows that Hall quasifields are not fields except in very small cases (actually only if $|F| = 2$).

Lemma 3. *If $m \in R - F$ then $f(m) = 0$.*

Algorithm 1, which follows [2, p. 364–365], shows how to solve the equation $xm = xn + v$ when $n \neq m$ in a Hall quasifield.

For $a \in F$ we indentify a and $(a, 0)$. The case when both m and n are in F is easy; see line 6. Assume $m \neq 0$. Then we can write any $y \in R$ in the form $y_1' + y_2'm$ for unique y_1' and $y_2' \in F$; see lines 12 and 13. The most difficult case is when both $m_2 \neq 0$ and $n_2 \neq 0$. Using the definition of multiplication (1) and Lemma 3 to calculate $m(a + bm)$ and expressing the result in the form $c + dm$, one obtains the identity

$$m(a + bm) = -a^2b^{-1} + rb^{-1}a - b^{-1}s + (r - a)m$$

Writing $n = a + bm$, $v = v_1 + v_2m$, $x = x_1 + x_2m$ the equation $xm = xn + v$ becomes

$$\begin{pmatrix} -a & a^2b^{-1} - ab^{-1}r - b^{-1}s + s \\ 1 - b & a \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

The determinant of this system can be written as

$$-b^{-1}(a^2 - ra(1 - b) - s(1 - b)^2)$$

If $b = 1$ then $a \neq 0$ as $m \neq n$ and the determinant is not zero in this case. If $b \neq 1$ then the determinant can be expressed as $b^{-1}(1 - b)^2 f(a/(1 - b))$, which is not zero because $f(x)$ is irreducible.

Because the right distributive law holds, to solve $mx = nx + v$ for $n \neq m$ it is enough to solve $mx = v$, for $m \neq 0$. If $m = (a, b)$ and $v = (c, d)$, then x is given by the following:

$$x = \begin{cases} (c/a, 0) & \text{if } ad - bc = 0 \text{ and } a \neq 0, \\ (d/b, 0) & \text{if } ad - bc = 0 \text{ and } a = 0, \\ (\frac{cd - rbc - sab}{ad - bc}, \frac{d^2 - rbd - sb^2}{ad - bc}) & \text{if } ad - bc \neq 0. \end{cases}$$

1 % Given $m = (m_1, m_2)$, $n = (n_1, n_2)$ and $v = (v_1, v_2)$
2 % in R with $m \neq n$.
3 **procedure** $solve(m, n, v)$
4 **if** $m_2 = 0$ **then**
5 **if** $n_2 = 0$ **then**
6 $v \circ ((m_1 - n_1)^{-1}, 0)$
7 **else**
8 $solve(n, m, -v)$
9 **endif**
10 **else**
11 % Write $v = (v'_1, 0) + m \circ (v'_2, 0)$.
12 $v'_1 \leftarrow v_1 - m_1 m_2^{-1} v_2$
13 $v'_2 \leftarrow m_2^{-1} v_2$
14 **if** $n_2 = 0$ **then**
15 $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} \leftarrow \begin{pmatrix} -n_1 & s \\ 1 & r - n_1 \end{pmatrix}^{-1} \begin{pmatrix} v'_1 \\ v'_2 \end{pmatrix}$
16 $(x'_1, 0) + (x'_2, 0) \circ m$
17 **else**
18 % Write $n = (a, 0) + m \circ (b, 0)$.
19 $a \leftarrow n_1 - m_1 m_2^{-1} n_2$
20 $b \leftarrow m_2^{-1} n_2$
21 $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} \leftarrow \begin{pmatrix} -a & a^2 b^{-1} - arb^{-1} - sb^{-1} + s \\ 1 - b & a \end{pmatrix}^{-1} \begin{pmatrix} v'_1 \\ v'_2 \end{pmatrix}$
22 $(x'_1, 0) + (x'_2, 0) \circ m$
23 **endif**
24 **endif**
25 **endprocedure**

Algorithm 1: Solving $xm = xn + v$.

Hanna's Quadrangles

If $r + s = 1$ then $f(1) = 0$, but $f(x)$ is irreducible. Thus let $k = (r + s - 1)^{-1}$.

All the incidences of Table 1 are easily seen to hold except for two. That $[(ks, k), -(ks, k), 1]$ is on $\langle (0, 1), 1, -(0, 1) \rangle$ requires the definition of k but does always hold. The second is covered in the next lemma.

Lemma 4. *$[(ks, k), 0, 1]$ is on $\langle (1, 1), 1, -(0, 1) \rangle$ if and only if $2s + r = 1$.*

In a plane with $2s+r = 1$ (note this implies $k = -s^{-1}$ we can use Hanna's quadrangle to introduce plus and times operations. Then 'adding one' will induce a permutation δ on the elements of one of the lines. Specifically we let $a_1 = [0, 0, 1]$, $a_2 = [0, 1, 0]$, $a_3 = [(-1, k), 0, 1]$, $c_{13} = [1, 0, 1]$, and $c_{23} = [(-1, k), (1, -k), 1]$. Any point on the line $a_1 \vee a_2$ except a_2 has the

TABLE 1. Hanna's quadrangle.

$\langle 1,0,0\rangle$	:	$[0,0,1]$	$[0,1,0]$	$[0,(0,1),1]$
$\langle 0,1,0\rangle$	:	$[0,0,1]$	$[1,0,1]$	$[(ks,k),0,1]$
$\langle 1,0,-(ks,k)\rangle$	:	$[0,1,0]$	$[(ks,k),0,1]$	$[(ks,k),-(ks,k),1]$
$\langle 1,1,0\rangle$	:	$[0,0,1]$	$[1,-1,1]$	$[(ks,k),-(ks,k),1]$
$\langle (1,1),1,-(0,1)\rangle$	:	$[1,-1,1]$	$[(ks,k),0,1]$	$[0,(0,1),1]$
$\langle (0,1),1,-(0,1)\rangle$	:	$[1,0,1]$	$[(ks,k),-(ks,k),1]$	$[0,(0,1),1]$
$\langle 1,0,-1\rangle$	:	$[0,1,0]$	$[1,0,1]$	$[1,-1,1]$

form $[0,(c,d),1]$. If we take this point and join it with a_3, then meet that line with $a_2 \vee c_{13}$, then join that point with c_{23}, then meet that line with $a_1 \vee a_2$, we obtain a point $[0,(c',d'),1]$. The map $(c,d) \mapsto (c',d')$ is a permutation of R given by

$$c' = \begin{cases} 2c^2 + c - 4cs & \text{if } c = sd, \\ \frac{-c^2-s-2cs+ds+2cds}{2(ds-c)} & \text{if } \det = 0, \\ \frac{-c^2+c^3-s+cs+2c^2s+ds+cds-4c^2ds-4ds^2-4cds^2+2d^2s^2+4cd^2s^2}{\det} & \text{if } \det \neq 0. \end{cases}$$

$$d' = \begin{cases} sd^2 - 2sd + 1 & \text{if } c = sd, \\ \frac{-1+d-cd-2ds+2d^2s}{ds-c} & \text{if } \det = 0, \\ \frac{-1+2c+d-2cd+c^2d-5ds+2cds+4d^2s-4cd^2s-4d^2s^2+4d^3s^2}{\det} & \text{if } \det \neq 0. \end{cases}$$

where

$$\det = c^2 - s + 2cs + ds - 4cds - 4ds^2 + 4d^2s^2.$$

Note if $\det = 0$ for (c,d) then $c' = sd'$.

Of course if the subplane generated by Hanna'a quadrangle and one other point on the line $a_1 \vee a_2$ is the whole plane then Hanna's Fano subplane is maximal. If we choose $\mathbf{F} = \mathbb{Z}/p\mathbb{Z}$ then the Hall plane has order p^2. By Baer's Theorem a proper subplane can have order at most p. So if a cycle of the permutation described above has size greater than p (actually $p-2$) then the sublattice generated by the quadrangle and a point from the cycle will generate the whole plane.

Now finding the cycle decomposition of this permutation for various values of p and all possible values of s exhibits the following properties:

- There are two 2–cycles: $(0,0) \leftrightarrow (0,1)$ and $(2s,1) \leftrightarrow (2s,2)$. The former is first cycle lexicographically, of course, and the latter is the last. In the examples checked, the quadrangle and the second 2–cycle generated the whole plane.
- Every other cycle has order at least $p+2$. For some values of s there are cycles of size $p+2$.
- The cycle length come in pairs except for one which may have odd length.

For example, with $p = 503$, $s = 23$ gives cycle lengths 2, 253005, and 2. With $s = 2$ the lengths are 2, 141897, 48993, 48993, 6056, 6056, 505, 505, and 2.

Define the *type* of an element (c, d) of R as follows. If $c = ds$ the type is 0; if det as defined above is 0 then (c, d) has type 1; otherwise it has type 2.

Lemma 5. *If (c, d) has type 1 then $(c', d') = \delta(c, d)$ has type 0. If (c, d) has type 0 then $(c', d') = \delta(c, d)$ has type 1 if and only if (c, d) is either $(0, 0)$ or $(2s, 2)$.*

Proof: If (c, d) has type 1 we use the formula for (c', d') above to evalulate $c' - d's$. This evaluates to det, which is 0 by assumption. If (c, d) has type 0 so $c = ds$, $\det(c', d')$ simplifies to $2s^2d(d - 2)$ so we must have $d = 0$ or 2 and the lemma follows.

References

[1] A. Albert and R. Sandler, *An introduction to finite projective planes*, Holt, Rinehart, and Winston, New York, 1968.
[2] M. Hall, *The theory of groups*, Chelsea, New York, 1959.
[3] D. Hughes and F. Piper, *Projective planes*, Graduate Texts in Math., vol. 6, Springer, Berlin, 1973.
[4] F. Stevenson, *Projective planes*, W. H. Freeman, San Francisco, 1972.

University of Hawaii, Honolulu, HI 96822
E-mail address: ralph@math.hawaii.edu