PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 4, Number 2/2003, pp.000-000.

ON COLLINEAR AND QUASI-COLLINEAR INVOLUTIONS

Richard GABRIEL

Hardtstr. 36, D-76185 Karlsruhe, Germany

We show that involution collinearity and involution quasi-collinearity are equivalent concepts in the projective group $P_1(F)$.

An element $i \neq e$ in a group with unity e is said to be an *involution* if $i^2 = e$.

Three involutions i_1, i_2, i_3, where at least two of them are different, are said to be *collinear* if their product also is an involution: $i_1\, i_2\, i_3 = i$. This definition was given by J.Hjemslev and G.Hessenberg; later Bachmann [1] used it in order to develop a plane geometry foundation based on group theory. In [2] we have investigated it in various groups and algebras, especially in symmetric groups.

Three involutions i_1, i_2, i_3 are said to be *quasi-collinear* if there exists an element $c \neq e$ such that the products

$$c\, i = i_1', c i_2 = i_2', c i_3 = i_3'$$

all are involutions. We have introduced this definition in [3] in connection with uniqueness of the solution to a three-message problem in a group.

Let F be a field and $P_1(F)$ the associated projective group; it consists of all homographies of F, i.e. of all maps of the form:

$$y = \frac{ax+b}{cx+d}, \quad x \in F,$$

with $a, b, c, d \in F$. Such a map can be homeomorphically represented by the matrix:

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then the product of two homographies corresponds to the products of the two associated matrices. An involution is characterized by $d = -a$ and $\det K \neq 0$.

Proposition. *For any three involutions* i_1, i_2, i_3 *in* $P_1(F)$ *the following statements are equivalent*:

(i) i_1, i_2, i_3 *are collinear*: $i_1\, i_2\, i_3 = i$;

(ii) i_1, i_2, i_3 *are quasi-collinear*: $c i = i_1', c i_2 = i_2', c i_3 = i_3', \ c \neq e$;

(iii) *the matrices*:

$$K_1 = \begin{bmatrix} x_1 & x_2 \\ x_3 & -x_1 \end{bmatrix}, \quad K_2 = \begin{bmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{bmatrix}, \quad K_3 = \begin{bmatrix} z_1 & z_2 \\ z_3 & -z_1 \end{bmatrix}$$

associated with the involutions i_1, i_2, i_3 *are linearly dependent*.

Proof. Obviously, (iii) is equivalent to

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} = 0 \qquad \text{(iv)}$$

We will show that both (i) and (ii) are equivalent to (iv). First, let us calculate the product

$$K_1 K_2 K_3 = \begin{bmatrix} x_1 & x_2 \\ x_3 & -x_1 \end{bmatrix} \begin{bmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{bmatrix} \begin{bmatrix} z_1 & z_2 \\ z_3 & -z_1 \end{bmatrix} =$$

$$= \begin{bmatrix} x_1 y_1 z_1 + x_2 y_3 z_1 + x_1 y_2 z_3 - x_2 y_1 z_3 & * \\ * & x_3 y_1 z_2 - x_1 y_3 z_2 - x_3 y_2 z_1 - x_1 y_1 z_1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Now it is clear that $a + d = 0$, that is, (i) is equivalent to (iv).

Second, let $C \neq \lambda I$ be a matrix with $\det C \neq 0$ consider the products

$$CK_1 = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & -x_1 \end{bmatrix} = \begin{bmatrix} c_1 x_1 + c_2 x_3 & * \\ * & c_3 x_2 - c_4 x_1 \end{bmatrix}$$

$$CK_2 = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \begin{bmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{bmatrix} = \begin{bmatrix} c_1 y_1 + c_2 y_3 & * \\ * & c_3 y_2 - c_4 y_1 \end{bmatrix}$$

$$CK_3 = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \begin{bmatrix} z_1 & z_2 \\ z_3 & -z_1 \end{bmatrix} = \begin{bmatrix} c_1 z_1 + c_2 z_3 & * \\ * & c_3 z_2 - c_4 z_1 \end{bmatrix}$$

These matrices are associated with involutions if and only if

$$\begin{aligned} (c_1 - c_4) x_1 + c_3 x_2 + c_2 x_3 &= 0 \\ (c_1 - c_4) y_1 + c_3 y_2 + c_2 y_3 &= 0 \\ (c_1 - c_4) z_1 + c_3 z_2 + c_2 z_3 &= 0 \end{aligned} \qquad \text{(v)}$$

and it is easy to see that (v) is equivalent to (iv).

Remarks.

1. Statement (ii) is a consequence of statement (i) even in an arbitrary group G. Indeed, from $i_1\, i_2\, i_3 = i$ we get

$$(i_1 i_2) i_3 = i = i_3', \; (i_1 i_2) i_2 = i_1 = i_2', \; (i_1 i_2) i_1 = i_1'.$$

With $c = i_1 i_2 \neq e$, statement (ii) is satisfied as soon as $i_1 \neq i_2$.

2. In a Bachmann geometry, the group $P_1(F)$ is essential. Therefore, collinearity and quasi-collinearity in $P_1(F)$ are equivalent concepts.

3. In an infinite symmetric group there are, however, quasi-collinear involutions which are not collinear.

REFERENCES

1. BACHMANN, F., *Aufbau der Geometrie aus dem Spiegelungsbegriff*. Berlin, 1959.
2. GABRIEL, R., *Eine Kollinearitätsbedingung für Involutionen in Gruppen und Algebren*. J. Reine Angew. Math. **267**, pp.20 – 49, 1974.
3. GABRIEL, R., *Three-message problem in a symmetric group with application to a cryptographic method*. Rev. Roumaine Math. Pures Appl. **45,** pp. 937 - 941, 2000.

Received February 26, 2003