CHAINS IN THE PROJECTIVE LINE

By A. J. Hoffman

Let E be a quadratic extension of a field F, let n be the projective line over E and $m \subset n$ be the projective line over F. Define a chain in n as the image of m under any projective transformation of n. In the classical case F is the real numbers, E the complex numbers, and the chains can be regarded as the circles of the real inversion plane. It is to be expected that many of the properties of chains in the classical case should hold in general. For example, the reader will readily see that the following facts, which we shall use freely in the remainder of the paper, are true:

(i) given three distinct points, there is one and only one chain containing them;

(ii) if p and q are points and c is a chain containing p but not q, then there is one and only one chain containing p and q and tangent to c (two chains are said to be tangent if their intersection consists of exactly one point).

We shall show that more interesting statements, such as Miquel's theorem and Von Staudt's theorem, are valid in the general case. The truth of Miquel's theorem has been known for some time [1; 70], but the following proof may be of interest since some of the lemmas were proved in a recent paper [4] for the special case $F = GF(p^{2^k})$. The symbol $(pq \cdots)$ means either "the points p, q, $\cdots$ are contained in a chain" or "the chain containing p, q, $\cdots$."

Miquel's Theorem. *Let p, q, r, s, t, u, v, w be distinct points such that $(pqrs)$, $(tuvw)$, $(pqtu)$, $(qruv)$, $(rsvw)$. Then $(pstw)$.*

Proof. If $(pqrs) = (tuvw)$, the theorem is immediate, so assume the contrary. We shall have to consider two cases.

Case I. E is a separable extension of F.

Then E admits an involutoric automorphism $\varphi: x \to \bar{x}$ having F as fixed field. If we define $\varphi: \infty \to \infty$, then φ is an involutoric mapping of n on itself such that $\varphi p = p$ if and only if $p \in m$. If H is the projective group of n and G is the group generated by H and φ, then H is of index 2 in G. Let $G - H$ be the set of all elements of G not in H.

Lemma 1. *Given a chain c, there is one and only one $\tau \in G - H$ leaving c pointwise fixed. Further, τ leaves no other point of n fixed and τ is an involution.*

Proof. Let $\rho \in H$ map m onto c. Define $\tau = \rho\varphi\rho^{-1}$; clearly τ fixes every point of c. If $\sigma \in G - H$ also has this property, then $\sigma^{-1}\tau \in H$ leaves at least three points fixed, since every chain contains at least three points; hence, [3; 95] $\sigma^{-1}\tau$

Received April 9, 1951. This work was done under a grant from the Office of Naval Research.