16. ELLIPTIC CURVES: FUNDAMENTAL ASPECTS.

The theory of elliptic curves over an arbitrary field K offers an appealing mixture of geometric and algebraic arguments. Let $\mathscr{C}$ be a non-singular cubic in PG(2,q). For the projective classification when K = GF(q), see [6] Chapter 11. Although $\mathscr{C}$ may have no inflexion, up to isomorphism it may be assumed to have one, O.

THEOREM 16.1: If $\mathscr{C}'$, $\mathscr{C}''$ are cubic curves in PG(2,K) such that the divisors $\mathscr{C}.\mathscr{C}' = \sum_{i=1}^{9} P_i$ and $\mathscr{C}.\mathscr{C}'' = \sum_{i=1}^{8} P_i + Q$, then $Q = P_9$.

Proof. (Outline) Through $P_1,\ldots,P_8$ there is a pencil $\mathscr{F}$ of cubic curves to which $\mathscr{C}$, $\mathscr{C}'$, $\mathscr{C}''$ belong. Any curve of $\mathscr{F}$ has the form $V(F+\lambda G)$ and so contains $V(F) \cap V(G)$. By Bézout's theorem $|V(F)\cap V(G)|=9$. Hence $Q = P_9$.

For a detailed proof, see [3], Chapter 5.

Theorem 16.1 is known as the theorem of the <u>nine associated points</u>. It has numerous corollaries of which we give a variety before the important theorem 16.7.

THEOREM 16.2: Any two inflexions of $\mathscr{C}$ are collinear with a third.

Proof. Let P_1, P_2 be inflexions of $\mathscr{C}$ with corresponding tangents ℓ_1, ℓ_2. Let $\ell = P_1P_2$ meet $\mathscr{C}$ again at P_3, and let ℓ_3 be the tangent at P_3 mecting $\mathscr{C}$ again at Q. Then

$$\mathscr{C}.\ell_1 = 3P_1, \quad \mathscr{C}.\ell_2 = 3P_2, \quad \mathscr{C}.\ell_3 = 2P_3+Q$$

$$\mathscr{C}.\ell = P_1 + P_2 + P_3 .$$

Hence

$$\mathscr{C}.\ell_1\ell_2\ell_3 = 3P_1 + 3P_2 + 2P_3 + Q$$

$$\mathscr{C}.\ell^3 \quad = 3P_1 + 3P_2 + 3P_3 \quad .$$

By the previous theorem, $Q = P_3$; so P_3 is an inflexion.

THEOREM 16.3. If P_1 and Q_1 are any two points of $\mathscr{C}$, the cross-ratio of the four tangents through P_1 is the same as the cross-ratio of the four tangents through Q_1.

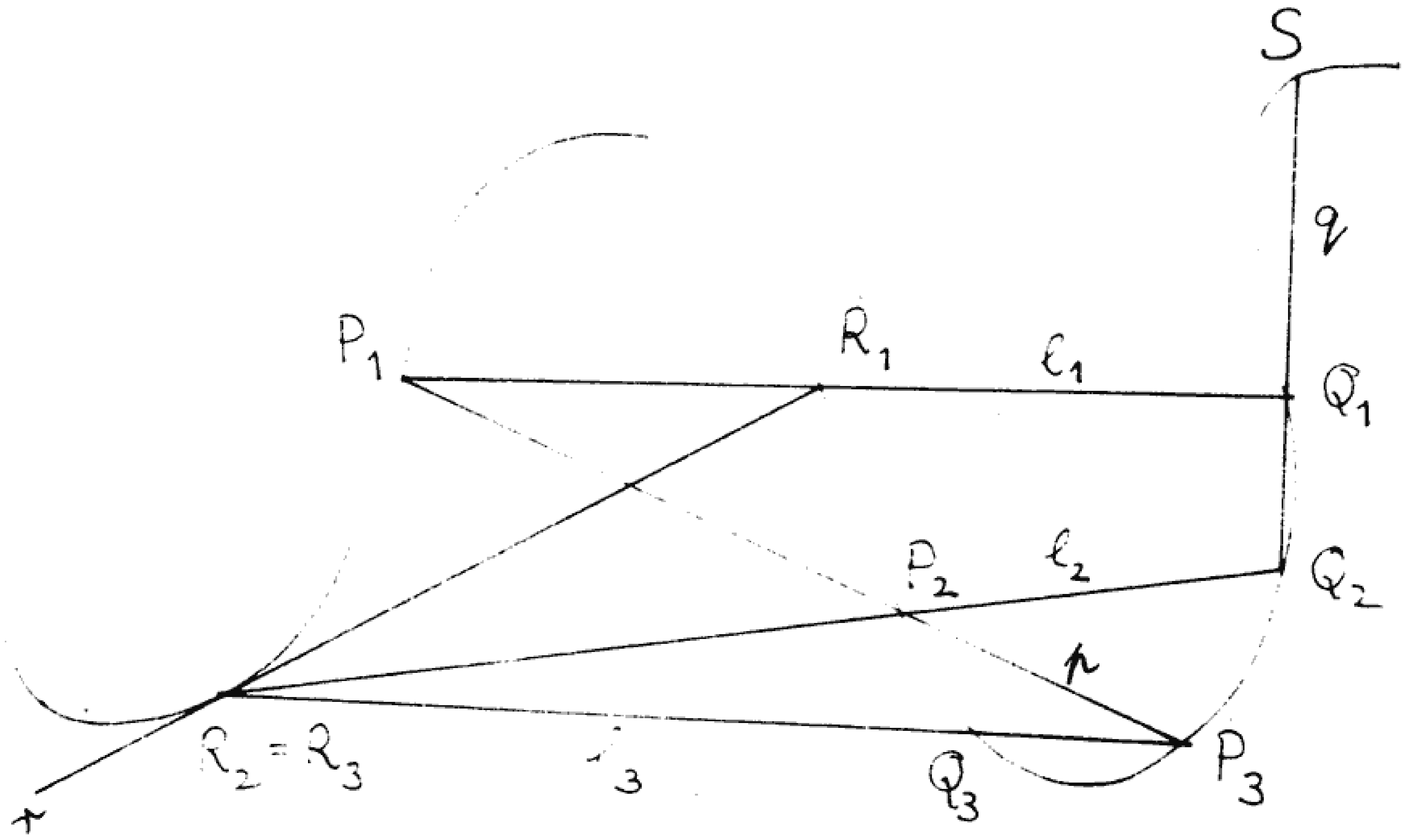
Proof. Let P_1Q_1 meet $\mathscr{C}$ again at R_1. Let r be a tangent to through R_1 with point of contact $R_2=R_3$. Let $P_1\ P_2\ P_3$ be any line through P_1 with P_2,P_3 on $\mathscr{C}$. Let R_2P_2 meet $\mathscr{C}$ again at Q_2 and let R_3P_3 meet $\mathscr{C}$ again at Q_3. We use the previous theorem to show that Q_1,Q_2,Q_3 are collinear.

Write $\quad \ell_i = P_iR_iQ_i$, $i=1,2,3$; let $p=P_1P_2P_3$, $r=R_1R_2$, $q=Q_1Q_2S$ with S the third point of Q on $\mathscr{C}$.

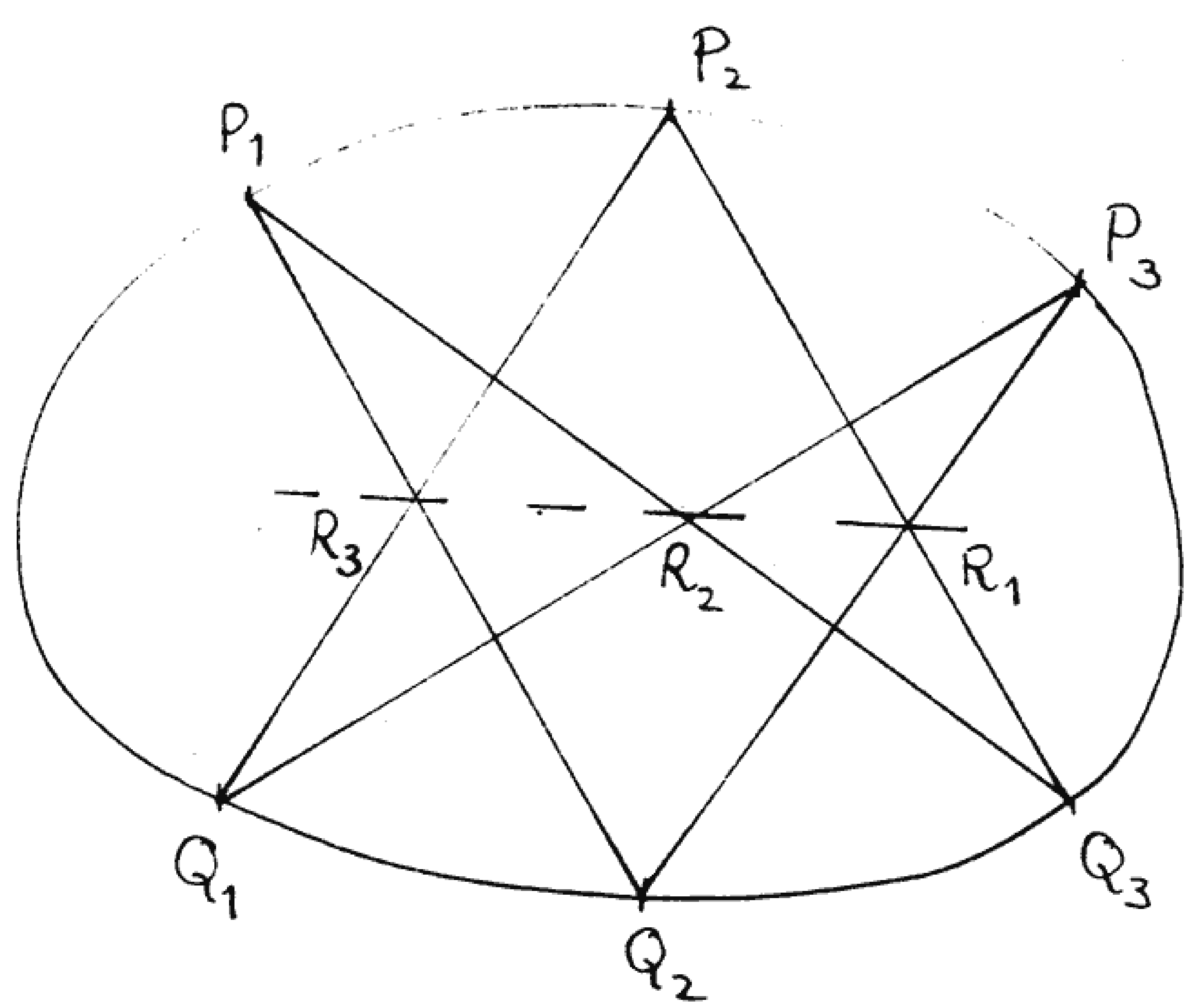
Then $\quad \mathscr{C}.\ell_1\ell_2\ell_3 = \sum_{i=1}^{3}(P_i+Q_i+R_i)$

$$\mathscr{C}.\ prq = \sum_{i=1}^{3} (P_i+R_i) + Q_1+Q_2+S.$$

Again by theorem 16.1, $S = Q_3$. When P_2 and P_3 coincide, so do Q_2 and Q_3. So there is an algebraic bijection τ from the pencil $\mathscr{F}$ through P_1 and the pencil G through Q_1 in which the tangents correspond. Hence τ is projective and the cross-ratios of the tangents are equal.



THEOREM 16.4. (Pascal's Theorem)



If $P_1Q_2P_3Q_1P_2Q_3$ is a hexagon inscribed in a conic $\mathscr{P}$,then the intersections of opposite sides, that is R_1,R_2,R_3, are collinear.

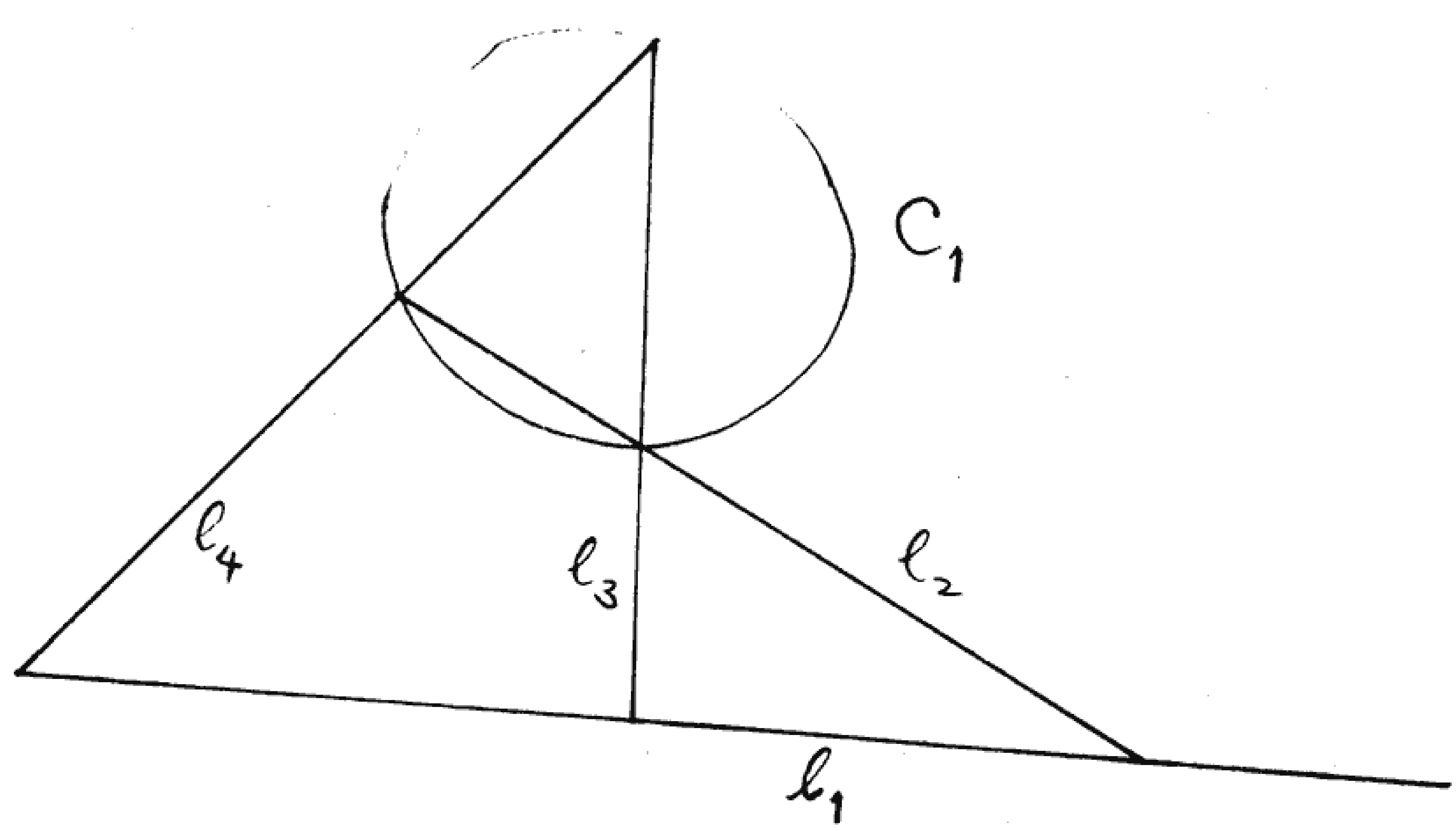
Proof. The two sets of three lines

$$P_1Q_2)(P_3Q_1)(P_2Q_3) \quad \text{and} \quad (Q_1P_2)(Q_3P_1)(Q_2P_3)$$

are cubics through the nine points P_i, Q_i, R_i, $i=1,2,3$; there is an irreducible cubic $\mathscr{C}$ in the pencil they determine. Also in the pencil is the cubic consisting of $\mathscr{P}$ and the line R_3R_2. So, by theorem 16.1, this cubic contains the ninth point R_1, which cannot lie on $\mathscr{P}$. So $R_3R_2R_1$ is a line.

THEOREM 16.5: Let $\ell_1, \ell_2, \ell_3, \ell_4$ be the sides of a complete quadrilateral in an affine plane and let C_i be the circumcircle of the triangle obtained by deleting ℓ_i. Then $C_1 \cap C_2 \cap C_3 \cap C_4 = \{P\}$.

Proof.



There is a pencil of cubics through the vertices of the quadrilateral and the two circular points at infinity. The four cubics $C_i + \ell_i$, $i=1,2,3,4$, contain these eight points and therefore the ninth associated point P. As each ℓ_i contains three of the eight initial points, it does not contain P. Hence P lies on each C_i.

Now we show that an elliptic curve $\mathscr{C}$ is an abelian group. As above we take O as an inflexion.

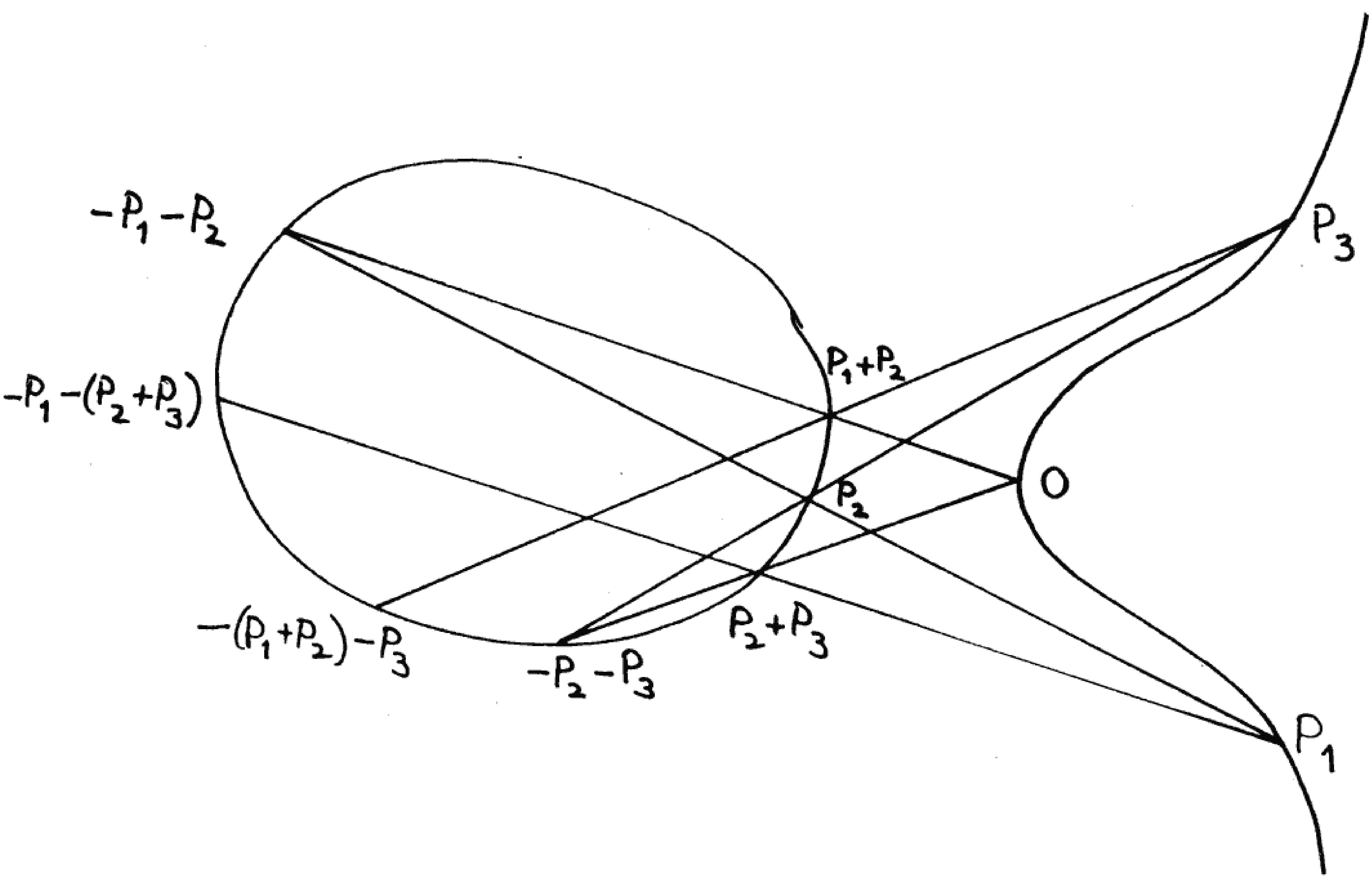
Definition: For P,Q on $\mathscr{C}$, let $\mathscr{C}.PQ=P+Q+R$ and let $\mathscr{C}.OR=O+R+S$; define $S = P+Q$.

LEMMA 16.6: (i) On $\mathscr{C}$, the points $O,P,-P$ are collinear.

(ii) P,Q,R are collinear on $\mathscr{C}$ if and only if $P+Q+R=O$.

THEOREM 16.7: Under the additive operation, $\mathscr{C}$ is an abelian group.

Proof. The only non-trivial property to verify is the associative law.



Apart from $\mathscr{C}$, consider the two cubics consisting of three lines given by the rows and columns of the array

$$\begin{array}{ccc} P_1 & P_2 & -P_1-P_2 \\ P_2+P_3 & P_2-P_3 & 0 \\ X & P_3 & P_1+P_2 \end{array}$$

Again, by theorem 16.1, X lies on both these cubics. So, $X = -P_1-(P_2+P_3) = -(P_1+P_2)-P_3$; hence, if Y is the third point of $\mathscr{C}$ on OX, then

$$Y = P_1+(P_2+P_3) = (P_1+P_2)+P_3.$$

Note: $\mathscr{C}$ has been drawn as $y^2=(x-a)(x-b)(x-c)$ with $a<b<c$, but the point of inflexion natural to this picture is at infinity.

THEOREM 16.8: (Waterhouse [21]). For any integer $N=q+1-t$ with $|t| \le 2\sqrt{q}$, there exists an elliptic cubic in PG(2,q), $q= p^h$, with precisely N rational points if and only if one of the following conditions on t and q is satisfied:

(i)	$(t,p) = 1$	
(ii)	$t = 0$	h odd or $p \not\equiv 1 \pmod 4$
(iii)	$t = \pm\sqrt{q}$	h even and $p \not\equiv 1 \pmod 3$
(iv)	$t = \pm 2\sqrt{q}$	h even
(v)	$t = \pm\sqrt{2q}$	h odd and $p = 2$
(vi)	$t = \pm\sqrt{3q}$	h odd and $p = 3$

COROLLARY:
$$N_q(1) = \begin{cases} q + [2\sqrt{q}] & \text{if } p \text{ divides } [2\sqrt{q}],\ h \text{ is odd and } h \ge 3; \\ q+1+[2\sqrt{q}] & \text{otherwise.} \end{cases}$$