CHARACTERIZATION OF MODULAR CORRESPONDENCES BY GEOMETRIC PROPERTIES

ALLAN ADLER

In this paper, we will show how certain Hecke correspondences on modular curves may be characterized by their geometrical properties. We introduce the notion of a cuspidal correspondence and of an almost unramified correspondence (Definition 5) and prove (Theorem 1) that an irreducible almost unramified cuspidal correspondence on a modular curve is a modular correspondence. By considering the bidegree and the invariance properties of the correspondence we are able to some extent to identify the correspondences which arise (cf. Theorem 2 of $\S4$). In $\S5$, we give some simple criteria which sometimes make it easier to show that a correspondence is cuspidal. It would be very useful to have similar criteria for a correspondence to be almost unramified. We illustrate the theory with nontrivial examples on the curves X(5) and X(7).

0. Introduction. In this paper, we will show how certain Hecke correspondences on modular curves may be characterized by their geometric properties. The study of the equations defining modular correspondences was initiated by Adolf Hurwitz, Felix Klein and Ernst Wilhelm Fiedler in the last century. In [H], Adolf Hurwitz obtained a general coincidence formula for correspondences on an algebraic curve and considered from a general point of view the number of equations needed to define a correspondence. In Ch. VI, 6 §6 of [K-F], Felix Klein obtained some explicit equations for modular correspondences and gave criteria for a correspondence to arise as a Schnittsystem-Correspondenz. Since then, this aspect of the theory of modular correspondences has been largely neglected in favor of more powerful and general analytic and number theoretic methods which do not involve explicit equations. Our methods are essentially different from those of these classical authors.

In the first section, we discuss correspondences in the category of covering spaces. While the results of §1 are certainly well known, it is convenient to include them for easy reference. In §2, we consider the different actions of the group $PSL_2(\mathbb{Z}/N\mathbb{Z})$ on the modular curve X(N) of level N. In §3, we introduce the notion of a cuspidal

1

correspondence and of an almost unramified correspondence (Definition 5) and prove (Theorem 1) that an irreducible almost unramified cuspidal correspondence on a modular curve is a modular correspondence. This is a very coarse result since it does not allow one to say which modular correspondence one is dealing with. By considering the bidegree and the invariance properties of the correspondence we are able to some extent to remedy this defect with Theorem 2 of §4. In §5, we give some simple criteria which sometimes make it easier to show that a correspondence is cuspidal. In §6, we present simple criteria for a correspondence to be almost unramified. Together with the criteria of §5, they provide an efficient technique for proving that a correspondence is a modular correspondence. One lacuna in our technique is that we have not discussed the precise action of modular correspondences on the cusps of X(N) in general. Knowledge of this action in a particular case may allow one to identify a modular correspondence when there is more than one correspondence of a given bidegree.

We also give nontrivial examples of the above theory in the case of the modular curves X(5) and X(7). In §7 we show that for r = 2, 3, the Hecke correspondences T_r are essentially defined by $\sum x_i = \sum x_i^2 = \sum x_i^{r+1} = 0$, where $\sum x_i = \sum x_i^2 = 0$ is identified with $X(5) \times X(5)$. In §8, we recall the geometry of the realizations of X(7) as the plane curve $X^3Y + Y^3Z + Z^3X = 0$ and as the jacobian curve of a net of quadrics in $P^3(C)$. To each point of the space curve there corresponds a trisecant, arising as the intersection of the polar planes of the point with respect to all of the quadrics in the net, and there are three trisecants through each point of the curve. In $\S 9$, we show that the Hecke correspondence T_2 on X(7) is essentially the correspondence on the space curve that associates to a point p the three points where the curve is met by the trisecant associated to $\,p$. The modular correspondence associated to the double coset $\Gamma(7)\eta^{-1}\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}\Gamma(7)$, for suitable η in $SL_2(\mathbf{Z})$, is the correspondence on the space curve that associates to a point p the six points other than pwhere the trisecants through p meet the curve. Working instead with the plane curve, we also recover the classical result of Klein which says that this correspondence is the correspondence on the plane which associates to each point p of the plane curve the six points, other than p, where the polar conic of the curve with respect to p meets the curve. An application of the theory to modular correspondences on X(11) will appear in [A]. In the case of X(11), the correspondences we obtain cannot arise as Schnittsystem-Correspondenzen and therefore are not accessible by the methods of Klein.

At the end of volume 2 of Klein-Fricke (cf. [K-F], [F]) one finds equations defining modular correspondences on some modular curves, especially X(7) and the Fermat curves $x^4 + y^4 + z^4 = 0$ and $x^8 + y^8 + z^8 = 0$. The classical results are impressive and the methods are apparently different from ours. We hope to study their methods more closely in a future paper. Another direction which we hope to investigate is the problem of generalizing the results of this article to other arithmetic groups.

The author is indebted to W. L. Edge, Steve Kleiman and Israel Vainsencher for helpful correspondence related to this article.

1. Correspondences in the category of covering spaces.

LEMMA 1. Let X_1 and X_2 be connected locally path connected semilocally simply connected spaces and let $g_i \colon Z_i \to X_i$ be universal covering spaces for i=1,2. Let Y be a subspace of $X_1 \times X_2$ and for i=1,2 let f_i denote the restriction to Y of the projection $X_1 \times X_2 \to X_i$. Assume that f_1 and f_2 are covering projections. Then the mapping $g \colon Z_1 \times Z_2 \to X_1 \times X_2$ defined by $g(z_1, z_2) = (g_1(z_1), g_2(z_2))$ is a universal covering projection. Furthermore, there is a homeomorphism α of Z_1 onto Z_2 such that the restriction of g to the graph of α is a universal covering space of Y.

Proof. By Corollary 2.5.15 of Spanier's book [Sp], the spaces Z_1 and Z_2 are simply connected. Therefore $Z_1 \times Z_2$ is simply connected. The map g is obviously a covering projection so by Corollary 2.5.7 of [Sp], g is a universal covering projection. By the universal properties of g_1 and g_2 , we can find maps $h_i: Z_i \to Y$ for i=1,2 such that $f_i \circ h_i = g_i$. By Lemma 2.5.1 of [Sp], the maps h_1 and h_2 are themselves covering projections and by Corollary 2.5.7 of [Sp], they are in fact universal covers. By Corollary 2.5.6 of [Sp], the maps h_1 and h_2 are isomorphic over Y, so there is a homeomorphsim α of Z_1 onto Z_2 such that $h_2 \circ \alpha = h_1$. Denote by Y' the graph of α . Denote by β_1 and β_2 the restrictions to Y' of the projections of $Z_1 \times Z_2$ onto Z_1 and Z_2 respectively. We then have that

$$\nu = g|Y' = (g_1 \circ \beta_1, g_2 \circ \beta_2) = (f_1 \circ h_1 \circ \beta_1, f_2 \circ h_2 \circ \beta_2)$$

= $(f_1 \circ h_1 \circ \beta_1, f_2 \circ h_1 \circ \beta_1)$

since $h_1 \circ \beta_1 = h_2 \circ \beta_2$. Therefore $\nu = \iota \circ (h_1 \circ \beta_1)$ where ι is the inclusion of Y into $X_1 \times X_2$. This shows that ν maps Y' onto Y

and that the mapping $Y' \to Y$ induced by ν is $h_1 \circ \beta_1$. Since h_1 is a universal covering projection and β_1 is a homeomorphism, we conclude that $h_1 \circ \beta_1$ is a universal covering projection.

Let W be a connected simply connected space and let Γ_1 and Γ_2 be two groups of homeomorphisms, each acting properly discontinuously on W. Let $X_1 = \Gamma_1 \setminus W$ and $X_2 = \Gamma_2 \setminus W$ denote the orbit spaces for Γ_1 and Γ_2 respectively. For i = 1, 2, denote by g_i the natural mapping of W onto X_i . By Theorem 2.6.7 and Corollary 2.5.7 of [Sp], the mappings g_1 and g_2 are universal covering projections. Suppose in addition that Y is a subspace of $X_1 \times X_2$ and denote by f_1 and f_2 the restrictions to Y of the projections of $X_1 \times X_2$ onto X_1 and X_2 respectively. Assume that f_1 and f_2 are covering projections. Then we can apply Lemma 1. In particular, taking $g = (g_1, g_2)$: $W \times W \rightarrow X_1 \times X_2$ as in Lemma 1, we have that g is a covering projection. Furthermore, there is a homeomorphism α of W onto itself such that g maps the graph Y' of α onto Y and realizes Y' as a universal covering space of Y. Denote by $\pi\colon Y'\to Y$ the universal covering projection induced by π . Our goal in this section is to describe the relation Y in terms of Γ_1 , Γ_2 and α .

Lemma 2. Let notations and conventions be as above. Let $Y^{\#}$ denote the preimage of Y in $W \times W$ under g. Then $Y^{\#}$ is the union over all (γ_1, γ_2) in Γ_1 , and Γ_2 of the graphs of the homeomorphisms $\gamma_2^{-1}\alpha\gamma_1$ of W onto itself. Furthermore, any two of the graphs are either disjoint or identical.

Proof. Since g maps Y' onto Y, it follows that every point of Y has a representative of the form $(w, \alpha w)$ with w in W. If (w_1, w_2) belongs to $Y^\#$ then we can find γ_1 in Γ_1 and γ_2 in Γ_2 such that $(\gamma_1w_1, \gamma_2w_2)$ belongs to Y', that is, such that $\gamma_2w_2=\alpha\gamma_1w_1$. But then (w_1, w_2) lies on the graph of $\gamma_2^{-1}\circ\alpha\gamma_1$, which proves the first assertion. In particular, for each (γ_1, γ_2) in $\Gamma_1\times\Gamma_2$, g maps the graph of $\gamma_2^{-1}\alpha\gamma_1$ onto Y and induces on that graph the covering projection $\pi\circ(\gamma_1, \gamma_2)$ onto Y. Now suppose that (γ_1, γ_2) and (γ_1', γ_2') belong to $\Gamma_1\times\Gamma_2$. Then the graphs of $\gamma_2^{-1}\alpha\gamma_1$ and $\gamma_2'^{-1}\alpha\gamma_1'$ are $(\gamma_1, \gamma_2)^{-1}Y'$ and $(\gamma_1', \gamma_2')^{-1}Y'$ respectively. Suppose these graphs meet each other at a point p. Let q be any point of $(\gamma_1, \gamma_2)^{-1}Y'$. Let σ be a path from p to q lying on $(\gamma_1, \gamma_2)^{-1}Y'$. Since g is a covering projection, σ is the unique lift of the path $g\circ\sigma$. On the other hand, $g\circ\sigma$ lies in

Y and $\pi \circ (\gamma_1', \gamma_2')$ is a covering projection from $(\gamma_1', \gamma_2')^{-1}Y'$ onto Y. So there is a lift τ of $g \circ \sigma$ to a path in $(\gamma_1', \gamma_2')^{-1}Y'$ beginning at p. Since the covering projection $\pi \circ (\gamma_1', \gamma_2')$ is the restriction to $(\gamma_1', \gamma_2')^{-1}Y'$ of g, it follows that σ and τ must coincide. In particular, $q = \sigma(1) = \tau(1)$ belongs to $(\gamma_1', \gamma_2')^{-1}Y'$. Therefore the graph of $\gamma_2^{-1}\alpha\gamma_1$ is contained in the graph of $\gamma_2'^{-1}\alpha\gamma_1'$. By symmetry of the above argument, the graphs coincide.

LEMMA 3. Retaining the assumptions and notation of Lemma 2, let A_1 denote the collection of all cosets $\Gamma_2 \alpha \gamma_1$ with γ_1 in Γ_1 and let A_2 denote the collection of all cosets $\Gamma_1 \alpha^{-1} \gamma_2$ with γ_2 in Γ_2 . Let w be any element of W. Define $\varphi_1 \colon A_1 \to Y$ and $\varphi_2 \colon A_2 \to Y$ by

$$\begin{aligned} \varphi_1(\Gamma_2\alpha\gamma_1) &= (\Gamma_1 w \,,\, \Gamma_2\alpha\gamma_1 w) \,, \\ \varphi_2(\Gamma_1\alpha^{-1}\gamma_2) &= (\Gamma_1\alpha^{-1}\gamma_2 w \,,\, \Gamma_2 w) \,. \end{aligned}$$

Let f_1 and f_2 denote, as in Lemma 1, the restrictions to Y of the projections $X_1 \times X_2 \to X_i$ for i = 1, 2. Then for i = 1, 2 the function φ_i maps A_i bijectively onto the fibre $f_i^{-1}(\Gamma_i w)$ of f_i over $\Gamma_i w$.

Proof. Since π maps Y' onto Y, every point of $f_1^{-1}(\Gamma_1 w)$ has a representative of the form $(\gamma_1 w, \alpha \gamma_1 w)$ with γ_1 in Γ_1 . It follows that every point of $f_1^{-1}(\Gamma_1 w)$ is of the form

$$g(\gamma_1 w, \alpha \gamma_1 w) = (\Gamma_1 w, \Gamma_2 \alpha \gamma_1 w) = \varphi(\Gamma_2 \alpha \gamma_1).$$

This shows that φ_1 is surjective. Similarly, every point of $f_2^{-1}(\Gamma_2 w)$ has a representative in Y' of the form $(\alpha^{-1}\gamma_2 w, \gamma_2 w)$ with γ_2 in Γ_2 . So every point of $f_2^{-1}(\Gamma_2 w)$ is of the form

$$g(\alpha^{-1}\gamma_2 w, \gamma_2 w) = (\Gamma_1 \alpha^{-1}\gamma_2 w, \Gamma_2 w) = \varphi_2(\Gamma_1 \alpha^{-1}\gamma_2).$$

Thus φ_2 is surjective. We will show that φ_1 is injective. The proof that φ_2 is injective is quite similar and is left to the reader. Suppose that γ_1 and γ_1' are elements of Γ_1 such that $\varphi_1(\Gamma_2\alpha\gamma_1)=\varphi_1(\Gamma_1\alpha\gamma_1')$. Then $\Gamma_2\alpha\gamma_1w=\Gamma_2\alpha\gamma_1'w$ and we can find an element γ_2 and Γ_2 such that $\gamma_2\alpha\gamma_1w=\alpha\gamma_1'w$. But then the graph of $\gamma_2\alpha\gamma_1$ meets the graph of $\alpha\gamma_1'$. By Lemma 2, these two graphs must therefore coincide. So $\gamma_2\alpha\gamma_1=\alpha\gamma_1'$ and hence $\Gamma_2\alpha\gamma_1=\Gamma_2\alpha\gamma_1'$. This proves that φ_1 is injective.

DEFINITION 1. Retain the notation of Lemma 3. The cardinality of A_1 is called the *left degree* of Y and is denoted $d_1(Y)$. Similarly, the cardinality of A_2 is called the *right degree* of Y and is denoted $d_2(Y)$. The pair $(d_1(Y), d_2(Y))$ is called the *bidegree* of Y.

LEMMA 4. We retain the notation and assumptions of Lemma 3. The left degree $d_1(Y)$ is equal to the index of $\alpha^{-1}\Gamma_2\alpha\cap\Gamma_1$ in Γ_1 . Similarly, the right degree $d_2(Y)$ is equal to the index of $\alpha\Gamma_1\alpha^{-1}\cap\Gamma_2$ in Γ_2 .

Proof. See Proposition 3.1 of Chapter 3 of Shimura's book [Sh]. The proof given there assumes that $d_1(Y)$ and $d_2(Y)$ are finite but doesn't actually use finiteness in any essential way.

REMARK. All of the results of this section remain valid with appropriate changes if one works in the category of \mathscr{C}^{∞} covering spaces, holomorphic covering spaces, covering spaces which are local isometries or covering spaces in any other reasonable category of spaces whose maps satisfy a condition depending only on local properties.

DEFINITION 2. In the notation of Lemma 3, we say that Y belongs to the double coset $\Gamma_2 \alpha \Gamma_1$ and we write $Y = [\Gamma_2 \alpha \Gamma_1]$.

Proposition 1. Let W be a simply connected space and let Γ_1 and Γ_2 be groups which act properly discontinuously on W. For i=1,2 let W_i denote the orbit space $\Gamma_i \setminus W$ for the action of Γ_i . Let V be a connected subspace of $X_1 \times X_2$ and for i=1,2 let f_i denote the restriction to V of the projection of $X_1 \times X_2$ onto X_i . Assume that f_1 and f_2 are both covering projections. Then there is a homeomorphism α of W onto itself such that V belongs to the double coset $\Gamma_1 \alpha \Gamma_1$ in the sense of Definition 2.

Proof. This follows at once from Definition 2, Lemmas 2 and 3 and the discussion preceding Lemma 2.

2. Actions of $PSL_2(\mathbf{Z}/N\mathbf{Z})$ on X(N). In this section, we will prove some results which will allow us, in later sections, to characterize certain algebraic correspondences on modular curves by their invariance properties. In order to establish these results, it is necessary to consider different actions of the group $PSL_2(\mathbf{Z}/N\mathbf{Z})$ on the modular curve of level N. We will begin this section by describing these actions and then turn to the study of correspondences. Throughout this section N will denote an integer ≥ 4 and G will denote the group $PSL_2(\mathbf{Z}/N\mathbf{Z})$. The upper half plane will be denoted \mathcal{H} and Γ will denote the group $SL_2(\mathbf{Z})$.

Let $\Gamma(N)$ denote the subgroup of $SL_2(\mathbf{Z})$ consisting of all matrices congruent to the identity matrix modulo N. Then $\Gamma(N)$ acts properly

discontinuously on \mathcal{H} and the orbit space for this action is denoted Y(N). One can compactify Y(N) by adding a finite number of points in such a way that one obtains a compact Riemann surface X(N). Furthermore, the action of G on Y(N) extends to an action of G on X(N).

DEFINITION 3. Denote by $\rho_0: G \to \operatorname{Aut}(X(N))$ the action of G on X(N) which we have just described. Then ρ_0 will be called the *natural action* of G on X(N).

We can obtain actions of G on X(N) by composing ρ_0 with automorphisms of the group G. In general, these actions are not isomorphic to the natural action. In fact, we have the following result.

LEMMA 5. Denote by A the group of automorphisms of G and by B the subgroup of A consisting of all inner automorphisms. Let σ belong to A. Then the action $\rho_0 \circ \sigma$ of G on X(N) is isomorphic to ρ_0 if and only if ρ_0 belongs to B.

Proof. If σ belongs to B, let g be an element of G such that $\sigma(x) = gxg^{-1}$ for all x in G. Then for all x in G we have

$$\rho_0 \circ \sigma(x) = \rho_0(gxg^{-1}) = \rho_0(g)\rho_0(x)\rho_0(g)^{-1},$$

which proves that ρ_0 and $\rho_0 \circ \sigma$ are isomorphic. Conversely, suppose that γ is an automorphism of X(N) such that

$$\rho_0 \circ \sigma(x) = \gamma \circ \rho_0(x) \gamma^{-1}$$

for all x in G. Then in particular γ normalizes the image of ρ_0 . Therefore γ acts on the orbit $G\setminus X(N)$, which is isomorphic to \mathbf{P}^1 . There are three distinguished points on $G\setminus X(N)$, namely the three branch points of the mapping $X(N)\to G\setminus X(N)$. The orders of ramification at these points are 2, 3 and N respectively. In particular, they are all distinct, so the action of γ on $G\setminus X(N)$ must fix these points. It follows that γ acts trivially on $G\setminus X(N)$. Therefore γ belongs to the image of ρ_0 . Let us say that $\gamma=\rho_0(g)$. Then for all x in G we have

$$\rho_0 \circ \sigma(x) = \gamma \circ \rho_0(x) \chi \gamma^{-1} = \rho_0(g \chi g^{-1}).$$

Since ρ_0 is faithful, we conclude that σ belongs to B.

From the natural action ρ_0 of G on X(N), we deduce an action of $G \times G$ on $X(N) \times X(N)$ which we call the *natural action* of $G \times G$ and which we will also denote by ρ_0 when no confusion can arise.

3. A coarse characterization of modular correspondences. For the rest of this paper, Ξ will denote an irreducible correspondence from the curve X(N) to itself. We will assume that Ξ is not of the form $\{x\} \times X(N)$ or $X(N) \times \{x\}$, where x is a point of X(N). The algebraic surface $X(N) \times X(N)$ has an involution ι which interchanges the two factors. If (x, y) is a point of this surface then we have $\iota(x, y) = (y, x)$. The image of Ξ under ι is called the *transpose* of Ξ and is denoted $\iota(\Xi)$. We say that Ξ is *symmetric* if Ξ is equal to its transpose. We will also use the notation ${}^t\Xi$ instead of $\iota(\Xi)$.

DEFINITION 4. Let f denote the mapping of Ξ onto X(N) induced by the projection of $X(N) \times X(N)$ onto its first factor. By a branch point of Ξ we mean a branch point of the mapping f. By a ramification point of Ξ we mean a ramification point of f.

REMARK. A point p is a branch point of a correspondence Ξ if and only if some coefficient of the divisor $\Xi(p)$ is greater than 1.

Let us recall that a point p of X(N) is called a *cusp* if and only if x does not belong to Y(N).

DEFINITION 5. We will say that the correspondence Ξ is almost unramified if every branch point of Ξ and every branch point of $\iota(\Xi)$ is a cusp. We will say that Ξ is cuspidal if both Ξ and its transpose $\iota(\Xi)$ leave invariant the set of cusps of X(N).

It is easy to see that Ξ is cuspidal if and only if Ξ and $\iota(\Xi)$ both leave Y(N) invariant. If Ξ is such, we denote by Ξ_0 the restriction of Ξ to Y(N). In other words, $\Xi_0 = \Xi \cap (Y(N) \times X(N))$ or, what is the same, $\Xi_0 = \Xi \cap (Y(N) \times Y(N))$.

Let $\binom{a\ b}{c\ d}$ be a 2×2 matrix with entries such that the determinant ad-bc of the matrix is positive and such that the greatest common divisor of the entries of the matrix is 1. Let α be the automorphism of $\mathscr H$ given by $\alpha(z)=(az+b)/(cz+d)$. Denote by $[\Gamma(N)\alpha\Gamma(N)]$ the correspondence on X(N) which belongs to the double coset $\Gamma(N)\alpha\Gamma(N)$ in the sense of Definition 2 of §1. The closure of $[\Gamma(N)\alpha\Gamma(N)]$ in $X(N)\times X(N)$ is an algebraic correspondence on X(N) which we denote $J_N(\alpha)$. Any correspondence on X(N) of the form $J_N(\alpha)$ is called a modular correspondence. We will often write $J\binom{a\ b}{c\ d}$ instead of $J_N(\alpha)$ when it is convenient to do so.

Theorem 1. Let Ξ be an irreducible correspondence on X(N) and suppose that Ξ is unramified and cuspidal. Then Ξ is a modular correspondence.

Proof. Denote by Ξ_0 the restriction of Ξ to Y(N). Since Ξ is the closure of Ξ_0 in $X(N) \times X(N)$, we will be done if we can show that Ξ_0 is the correspondence $[\Gamma(N)\alpha\Gamma(N)]$ associated to the double coset $\Gamma(N)\alpha\Gamma(N)$ for a suitable automorphism of $\mathscr H$ as above.

Let f_1 and f_2 be the restrictions to Ξ_0 of the projections of $Y(N) \times Y(N)$ onto the first and second factors respectively. Let d_1 be the degree of f_1 and let d_2 be the degree of f_2 . Since Ξ is an algebraic correspondence, the degrees d_1 and d_2 are both finite. Since Ξ is both cuspidal and unramified, the maps f_1 and f_2 are covering projections and Ξ_0 is a smooth curve on $Y(N) \times Y(N)$. We can therefore apply the results of §1. Taking $W = \mathcal{H}$, $\Gamma_1 = \Gamma_2 = \Gamma(N)$ and $V = \Xi_0$ in Proposition 1 of §1, we conclude that there is an analytic automorphism α of \mathcal{H} such that Ξ_0 belongs to the double coset $\Gamma(N)\alpha\Gamma(N)$ in the sense of Definition 2 of §1. Since d_1 and d_2 are finite, we conclude from Lemma 4 of §1 that $\alpha\Gamma(N)\alpha^{-1}\cap\Gamma(N)$ and $\alpha^{-1}\Gamma(N)\alpha\cap\Gamma(N)$ both have finite index in $\Gamma(N)$. Since $\Gamma(N)$ has finite index in Γ , we can apply Lemma 3.10 of Shimura's book [Sh] as well as the discussion of commensurators at the beginning of §3.1 of [Sh] to conclude that α is an automorphism of \mathcal{H} of the form $\alpha(z) = (az + b)/(cz + d)$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a 2×2 integer matrix with positive determinant and with the greatest divisor of a, b, c and d equal to 1. Referring to the definition of modular correspondence given above, we are done.

4. Characterization of particular modular correspondences.

DEFINITION 6. Let Ξ be a correspondence of X(N) and let ρ_0 denote the natural representation of $G \times G$ on $X(N) \times X(N)$. By the *stabilizer* of Ξ we mean the subgroup of $G \times G$ consisting of all (g_1, g_2) in $G \times G$ such that the automorphism $\rho(g_1, g_2)$ of $X(N) \times X(N)$ leaves Ξ invariant. We will denote the stabilizer of Ξ by $S(\Xi)$.

One can view a correspondence Ξ on X(N) as a multiple-valued function from X(N) to itself. From that point of view, an element (g_1, g_2) of $G \times G$ belongs to $S(\Xi)$ if and only if

$$\rho_0(g_2)\circ\Xi=\Xi\circ\rho_0(g_1).$$

If Ξ is the modular correspondence $J_N(\alpha)$ associated to an automorphism α of $\mathscr H$ then (g_1,g_2) belongs to $S(\Xi)$ if and only if in $PSL_2(\mathbf Q)$ we have

(1)
$$\gamma_2 \Gamma(N) \alpha \Gamma(N) = \Gamma(N) \alpha \Gamma(N) \gamma_2$$

where for $i = 1, 2, \gamma_i$ is a representative in $PSL_2(\mathbf{Z})$ of g_i .

Lemma 6. Let Ξ be a modular correspondence of X(N). If the stabilizer of Ξ contains the graph of an automorphism φ of G then Ξ is of the form $J_N(\alpha)$, where the automorphism α of $\mathscr H$ is associated to a 2×2 integer matrix $\binom{a}{c}\binom{b}{d}$ with a, b, c and d relatively prime and with positive determinant relatively prime to N.

Proof. Since Ξ is a modular correspondence, we can write Ξ in the form $J_N(\alpha)$ where α is the automorphism associated to a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries with greatest common divisor 1 and positive determinant. Let (g_1, g_2) be an element of the stabilizer of Ξ and for i=1, 2 let γ_i be a representative of g_i in $\mathrm{PSL}_2(\mathbf{Z})$. Then we have

$$\gamma_2 \Gamma(N) \alpha \Gamma(N) = \Gamma(N) \alpha \Gamma(N) \gamma_1$$

in $PSL_2(\mathbf{Q})$. We can then lift γ_1 and γ_2 to elements $\overline{\gamma}_1$ and $\overline{\gamma}_2$ of Γ such that in $M_2(\mathbb{Z})$ we have

$$\overline{\gamma}_2\Gamma(N)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma(N) = \Gamma(N)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma(N)\overline{\gamma}_1 \,.$$

Let p be a prime dividing N. Reducing this identity modulo p, we have

$$\overline{\gamma}_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overline{\gamma}_1$$

in $M_2(\mathbf{F}_p)$. Since the elements of $\mathrm{SL}_2(\mathbf{F}_p)$ generate $M_2(\mathbf{F}_p)$ as an additive group, the above identity implies that the left ideal j generated by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $M_2(\mathbf{F}_p)$ is in fact two sided. Since $M_2(\mathbf{F}_p)$ is a simple ring and since the greatest common divisor of the entries a, b, c and d is 1, it follows that j is all of $M_2(\mathbf{F}_p)$ or, what is the same, the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is prime to p. Since p was an arbitrary prime divisor of N, it follows that the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is relatively prime to N.

LEMMA 7. Let $\xi = \binom{a\ b}{c\ d}$ be a 2×2 matrix whose entries are integers with greatest common divisor 1 and whose determinant is a positive integer D. Assume that N and D are relatively prime. Let α denote the automorphism of $\mathscr H$ given by $\alpha(z) = (az+b)/(cz+d)$. Let g denote the element of $PGL_2(\mathbf Z/N\mathbf Z)$ represented by the matrix ξ . Let g be the automorphism of g given by $g = gxg^{-1}$ for all g in g. Then the stabilizer of g is the graph of g.

Proof. Let x be an element of G and let γ_1 and γ_2 be representatives in $PSL_2(\mathbf{Z})$ of x and $\varphi(x)$ respectively. Let $\overline{\gamma}_1$ be a representative of γ_1 in Γ . We can then choose a representative $\overline{\gamma}_2$ of γ_2

in Γ such that

$$\overline{\gamma}_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overline{\gamma}_1$$

modulo N. We obviously have

$$\Gamma \overline{\gamma}_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma = \Gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overline{\gamma}_1 \Gamma,$$

so by Lemma 3.29(2) of [Sh], we have

$$\Gamma(N)\gamma_2\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma(N) = \Gamma(N)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\gamma_1\Gamma(N)$$

in $M_2(\mathbf{Z})$. Therefore in $PSL_2(\mathbf{Q})$ we have

$$\gamma_2\Gamma(N)\alpha\Gamma(N) = \Gamma(N)\alpha\Gamma(N)\gamma_1$$

and therefore

$$\varphi(x) \circ J_N(\alpha) = J_N(\alpha) \circ x$$
.

This shows that the stabilizer of $J_N(\alpha)$ contains the graph of φ . Conversely, suppose that (g_1, g_2) lies in the stabilizer of $J_N(\alpha)$ and let γ_1 and γ_2 be elements of $PSL_2(\mathbf{Z})$ representing g_1 and g_2 respectively such that

$$\gamma_2 \Gamma(N) \alpha \Gamma(N) = \Gamma(N) \alpha \Gamma(N) \gamma_1$$
.

Reducing modulo N we have in $PGL_2(\mathbb{Z}/N\mathbb{Z})$ that

$$g_2\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} g_1,$$

and therefore $g_2 = \varphi(g_1)$.

For every positive integer D, let $\psi(D) = D \cdot \prod (1 + \frac{1}{p})$ where the product runs over all primes p dividing D.

LEMMA 8. Let $\xi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 integer matrix with relatively prime entries and positive determinant D. Let δ denote the largest factor of D which is relatively prime to N. Let α be the automorphism of $\mathscr H$ given by $\alpha(z) = (az + b)/(cz + d)$. Then the bidegree of the modular correspondence $J_N(\alpha)$ is (n, n), where

$$n = \frac{\psi(ND)}{\psi(N)} = \frac{D}{\delta} \cdot \psi(\delta).$$

Proof. The double coset $\Gamma \xi \Gamma$ is a disjoint union of double cosets $\Gamma(N)\xi_i\Gamma(N)$ which are permuted by multiplication on the left or right by elements of Γ and therefore all of the double cosets $\Gamma(N)\xi_i\Gamma(N)$ induce correspondences of the same bidegree (n, n). On the other

hand, the double coset $\Gamma\xi\Gamma$ is equal to the double coset $\Gamma\begin{pmatrix}D&0\\0&1\end{pmatrix}\Gamma$ by the theory of elementary divisors. Therefore, the number n depends only on the numbers N and D and not on the entries of the matrix Ξ . In particular, we may assume that ξ is the matrix $\binom{D\ 0}{0\ 1}$. By Lemma 3 of §1, the right degree of $J_N(\alpha)$ is the number of cosets $\Gamma(N)\alpha_j$ in the double coset $\Gamma(N)\alpha\Gamma(N)$. By Proposition 3.1 of [Sh], this number is equal to the index of $\alpha^{-1}\Gamma(N)\alpha\cap\Gamma(N)$ in $\Gamma(N)$. Let us write H to denote the group $\alpha^{-1}\Gamma(N)\alpha\cap\Gamma(N)$. Then H consists of all matrices $\binom{w\ x}{y\ z}$ in $\Gamma(N)$ such that $x\equiv 0\pmod{DN}$. We want to compute the index $\Gamma(N)$ of $\Gamma(N)$. We have

$$\Gamma(ND) \subset H \subset \Gamma(N) \subset \Gamma$$

and therefore

(2)
$$(\Gamma(N):H) = \frac{(\Gamma(N):\Gamma(ND))}{(H:\Gamma(ND))} = \frac{(\Gamma:\Gamma(ND))}{(\Gamma:\Gamma(N))\cdot (H:\Gamma(ND))} .$$

For every positive integer M, denote by $\mathcal{F}(M)$ the subgroup of $\mathrm{SL}_2(\mathbf{Z}/M\mathbf{Z})$ consisting of lower triangular matrices. Then $\mathcal{F}(M)$ is a group of order $M \cdot \phi(M)$, where ϕ denotes the Euler ϕ function. There is a homomorphism π of $\mathcal{F}(ND)$ onto $\mathcal{F}(N)$ obtained by reducing the entries of a matrix modulo N and it is easy to see that this homomorphism is surjective. Furthermore, we have a homomorphism v of the group H onto the kernel of π given by reducing the entries of a matrix in H modulo ND. Evidently the kernel of v is $\Gamma(ND)$. Therefore, the index $(H:\Gamma(ND))$ of $\Gamma(ND)$ in H is equal to the order of the kernel of π , and since π is surjective we have

(3)
$$(H:\Gamma(ND)) = \circ(\ker \pi) = \frac{\circ(\mathscr{T}(ND))}{\circ(\mathscr{T}(N))} = \frac{ND \cdot \phi(ND)}{N \cdot \phi(N)}.$$

On the other hand, for every positive integer M we have

(4)
$$(\Gamma : \Gamma(M)) = M \cdot \phi(M) \cdot \psi(M)$$

combining equations (2), (3) and (4) we have

$$\begin{split} (\Gamma(N):H) &= \frac{ND \cdot \phi(ND) \cdot \psi(ND)}{N \cdot \phi(N) \cdot \psi(N)} \cdot N \\ &\quad \cdot \frac{\phi(N)}{ND \cdot \psi(ND)} = \frac{\psi(ND)}{\psi(N)} = \frac{D}{\delta} \cdot \psi(\delta) \end{split}$$

where δ is the largest divisor of D which is prime to N. This proves that the right degree of $J_N(\alpha)$ is equal to $\frac{D}{\delta} \cdot \psi(\delta)$. A similar argument, which we leave to the reader, shows that the left degree of $J_N(\alpha)$ is also equal to $\frac{D}{\delta} \cdot \psi(\delta)$, and the lemma is proved.

LEMMA 9. Let ξ be as in Lemma 7. Then we can write the double coset $\Gamma(N)\xi\Gamma(N)$ in the form $\Gamma(N)\eta\begin{pmatrix}D&0\\0&1\end{pmatrix}\Gamma(N)$ where η belongs to Γ .

Proof. By Lemma 7, there is an automorphism φ of G whose graph in $G \times G$ is the stabilizer of $J_N(\xi)$. For every g in G, let \overline{g} be a representative of g in Γ . Then as g runs over G, so does $\varphi(g)$. Therefore

$$\begin{split} \Gamma \cdot \Gamma(N) \xi \Gamma(N) &= \bigcup_{g \in G} \pm \overline{g} \Gamma(N) \xi \Gamma(N) \\ &= \bigcup_{g \in G} \pm \Gamma(N) \xi \Gamma(N) \varphi(g) \\ &= \Gamma(N) \xi \Gamma. \end{split}$$

Hence we have

$$\Gamma \xi \Gamma = \Gamma \cdot \Gamma(N) \xi \Gamma = \Gamma \cdot \Gamma \xi \Gamma(N) = \Gamma \xi \Gamma(N)$$
.

We know from the theory of elementary divisors that

$$\Gamma \xi \Gamma = \Gamma \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} \Gamma$$

SO

$$\begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} = \eta^{-1} \xi \lambda$$

where η belongs to Γ and λ belongs to $\Gamma(N)$. We then have

$$\Gamma(N)\xi\Gamma(N) = \Gamma(N)\eta \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} \lambda^{-1}\Gamma(N)$$
$$= \Gamma(N)\eta \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} \Gamma(N)$$

which proves the lemma.

LEMMA 10. Let ξ be as in Lemma 9. If the stabilizer of $J_N(\xi)$ is the diagonal of $G \times G$ then D is a quadratic residue modulo N. Furthermore, we can find a solution x of $x^2D \equiv 1 \pmod{N}$ such that

$$\Gamma(N)\xi\Gamma(N)=\Gamma(N)\eta\begin{pmatrix}D&0\\0&1\end{pmatrix}\Gamma(N)$$

where η is an element Γ congruent to $\pm \begin{pmatrix} x & 0 \\ 0 & xD \end{pmatrix}$ modulo N.

Proof. Since the diagonal of $G \times G$ stabilizes $J_N(\xi)$, we have modulo N that

$$\gamma \alpha \equiv \alpha \gamma$$

for all γ in G. Therefore $\alpha = \eta \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix}$ is congruent to a scalar matrix and η is congruent to a matrix of the form $\begin{pmatrix} x & 0 \\ 0 & xD \end{pmatrix}$. Since η has determinant 1, we have

$$x^2D \equiv 1 \pmod{N}.$$

In particular, D is a quadratic residue modulo N.

We summarize the results of Theorem 1, Lemma 6, Lemma 8 and Lemma 10 in the following theorem.

THEOREM 2. Let $N \ge 4$ and let Ξ be a correspondence of bidegree (n, n) on X(N). Suppose that Ξ has the following properties:

- (1) Ξ is cuspidal and almost unramified.
- (2) The stabilizer of Ξ is the diagonal of $G \times G$.
- (3) There is one and only one positive integer D relatively prime to N such that $n = \psi(D)$.

Then we can find a solution x of $x^2D \equiv 1 \pmod{N}$ such that

$$\Xi = J_N \left(\eta \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} \right) \, ,$$

where η is an element of Γ which is congruent to $\pm \begin{pmatrix} x & 0 \\ 0 & xD \end{pmatrix}$ modulo N.

For the more general situation where the stabilizer of Ξ is not necessarily the diagonal of $G \times G$, one can in practice use Lemma 7 instead of Lemma 10. If the correspondence is not stabilized by the graph of an automorphism of G, then we can use Lemma 8 and Theorem 1 to good advantage. We also note that in case condition (3) of Theorem 2 does not hold, one can often distinguish among the possible choices for D by considering the action of Ξ on the cusps of X(N).

5. Criteria for cuspidal correspondences. In this section we present some simple criteria for a correspondence to be cuspidal. While they are not necessary conditions, they are often useful in practice.

Lemma 11. Let Ξ be a correspondence of X(N) of bidegree (m, n) and suppose that the stabilizer of Ξ contains the graph of an automorphism φ of G. If N is prime and greater than both m and n then Ξ is cuspidal.

Proof. A point x of X(N) is a cusp if and only if x is fixed by an element γ of order N in G. When x and y are such, the divisor

 $\Xi(x)$ of order n on X(N) is fixed by $\varphi(\Gamma)$. It is therefore a sum of the orbits of the cyclic group $\langle \varphi(\gamma) \rangle$ of prime order N. Since the degree of $\Xi(x)$ is n < N, all of these orbits are singletons. So $\Xi(x)$ consists of cusps. Replacing Ξ by its transpose $\iota(\Xi)$ and φ by φ^{-1} , we have that $\iota(\Xi)$ also maps cusps to cusps. Therefore Ξ is cuspidal.

COROLLARY. Let K be a correspondence on X(N) of bidegree (m,n). We allow K to be reducible. Suppose that the stabilizer of K is the graph of an automorphism φ of G. If N is prime and greater than both m and n, then every irreducible component of K is stabilized by the graph of φ and is cuspidal.

Proof. Let Ξ be an irreducible component of K and suppose that Ξ has bidegree (a,b). Then $a \leq m$ and $b \leq n$. So N is greater than both a and b. Let Λ denote the graph of φ and let H be the subgroup of Λ which leaves Ξ invariant. If $H \neq \Lambda$ then H must have index $\geq N$ in Λ . Therefore, we can find $\lambda_1, \ldots, \lambda_N$ in Λ such that the images Ξ_1, \ldots, Ξ_N of Ξ under $\lambda_1, \ldots, \lambda_N$ are all distinct. Since K is invariant under Λ , it follows that each Ξ_i is a component of K. Therefore the bidegree of K satisfies $m \geq Na$ and $n \geq Nb$, contradicting our assumption that m and n are less than N. Therefore $H = \Lambda$ and by Lemma 11 we conclude that Ξ is cuspidal.

6. Criteria for almost unramified correspondences. In this section, we give a necessary and sufficient condition for a correspondence to be almost unramified. It is quite useful in practice.

LEMMA 12. Let Ξ be an irreducible (α, β) correspondence from a curve \mathscr{C}_1 to a curve \mathscr{C}_2 and suppose that Ξ has no component of the form $\{x\} \times \mathscr{C}_2$ with x in \mathscr{C}_1 or of the form $\mathscr{C}_1 \times \{y\}$ with y in \mathscr{C}_2 . Let p be a point of \mathscr{C}_1 . Then $\Xi(p)$ contains a branch point of the transpose ${}^t\Xi$ of Ξ if and only if p is a fixed point of the correspondence Θ defined by

$$\Theta = {}^{t}\Xi \circ \Xi - \alpha \Xi.$$

Proof. We can write

where the q_i are distinct points of \mathcal{E}_2 and where the a_i are positive integers such that

$$(6.3) \sum_{i=1}^{r} a_i = \alpha.$$

For $1 \le i \le r$, we can write

(6.4)
$${}^{t}\Xi(q_{i}) = c_{i}p + \sum_{j=1}^{s_{i}} b_{ij}p_{ij},$$

where ${}^{t}\Xi$ denotes the transpose of Ξ , where the p_{ij} are distinct points of \mathscr{C}_{1} for $1 \leq j \leq s_{i}$ and are different from p, and where c_{i} and the b_{ij} are positive integers such that

(6.5)
$$c_i + \sum_{i=1}^{s_i} b_{ij} = \beta.$$

If we compose Ξ and ${}^{t}\Xi$ at p, we obtain

(6.6)
$${}^{t}\Xi \circ \Xi(p) = \sum_{i=1}^{r} a_{i}{}^{t}\Xi(q_{i}) = \left(\sum_{i=1}^{r} a_{i}c_{i}\right)p + \sum_{i=1}^{r} \sum_{j=1}^{s_{i}} a_{i}b_{ij}p_{ij}.$$

Since the c_i are positive, equation (6.3) implies that

$$(6.7) \sum_{i=1}^{r} a_i c_i \ge \alpha.$$

Since we have not yet made any assumptions about p, this says that the correspondence ${}^t\Xi \circ \Xi$ contains the identity correspondence at least α times. Then p is a fixed point of the correspondence Θ if and only if the inequality (6.7) is strict. By equation (6.3), the inequality (6.7) is strict if and only if one of the c_i is greater than 1, or, what is the same, if and only if one of the q_i is a branch point of the transpose ${}^t\Xi$ of Ξ . This proves the lemma.

COROLLARY 1. Let Ξ be an irreducible cuspidal (α, β) correspondence on the modular curve X(N) and let Θ denote the correspondence ${}^t\Xi \circ \Xi - \alpha \Delta$. If every fixed point of Θ is a cusp then every branch point of ${}^t\Xi$ is a cusp.

Proof. Let q be a branch point of ${}^{t}\Xi$ and let p be a point of X(N) such that $\Xi(p)$ contains q. By Lemma 12, the point p is a

fixed point of Θ and therefore by hypothesis p is a cusp. Since the correspondence Ξ is cuspidal, it follows that every point of $\Xi(p)$ is a cusp as well. In particular, q is a cusp.

COROLLARY 2. Let Ξ be an irreducible cuspidal symmetric (α, α) correspondence on X(N) and let Θ denote the correspondence $\Xi \circ \Xi - \alpha \Delta$. If every fixed point of Θ is a cusp then Ξ is a modular correspondence.

Proof. This follows at once from Corollary 1, from the symmetry of Ξ and from Lemma 12.

REMARK. Sometimes one can also prove that a correspondence is almost unramified by using the Riemann-Hurwitz relation.

7. Some modular correspondence on X(5). In this, we apply the theory we have developed to obtain geometric characterizations of certain modular correspondences on the modular curve X(5). In particular, we are able to obtain descriptions of the Hecke correspondences T_2 and T_3 in Theorem 3 and Theorem 4 respectively. The relevant geometry was certainly considered by Klein [K] but he apparently never considered its application to modular correspondences on X(5).

We begin with the following well-known result.

LEMMA 13. The groups S_5 and $PGL_2(\mathbf{F}_5)$ are isomorphic. Any isomorphism between them carries A_5 onto $PSL_2(\mathbf{F}_5)$.

Proof. The second assertion is an easy consequence of the first. On the other hand, it is well known that A_5 and $PSL_2(\mathbf{F}_5)$ are isomorphic since both are simple groups of order 60. The group of automorphisms of A_5 is S_5 and there is a faithful homomorphism of $PGL_2(\mathbf{F}_5)$ into the automorphism group of $PSL_2(\mathbf{F}_5)$. It follows that S_5 is isomorphic to $PGL_2(\mathbf{F}_5)$ since both groups have the same order.

Using Lemma 1, we can view A_5 as a group of automorphisms of X(5). If $\gamma \in A_5$ and $x \in X(5)$, the image of x under γ will be denoted $\gamma \cdot x$. We can also view $A_5 \times A_5$ as a group of automorphisms of $X(5) \times X(5)$. Let σ be an element of S_5 which does not lie in A_5 and for γ in A_5 , let us write γ^{σ} to denote $\sigma \gamma \sigma^{-1}$. Let $G \subseteq A_5 \times A_5$ denote the graph of the automorphism $\gamma \mapsto \gamma^{\sigma}$ of A_5 .

Let $\Delta \subseteq X(5) \times X(5)$ denote the graph of the identity mapping of X(5). Although Δ is not invariant under G, the sheaf $\mathcal{O}(\Delta)$ is

invariant under G. The group G therefore acts on the four dimensional space V of sections of $\mathcal{O}(\Delta)$ and we have a G-equivariant embedding of G into the projective space $\mathbf{P}(V^*)$. The image will be a G-invariant quadric which we will denote by Q. In the proof of Theorem 3, we will show how to choose σ appropriately.

In order to carry out explicit computations, it is convenient to introduce some coordinates in V^* .

LEMMA 14. Let S be a five element set on which G acts transitively. Then V^* is G-equivariantly isomorphic to the space of all functions $f: S \to \mathbb{C}$ such that $\sum f(s) = 0$, where the summation runs over all elements s of S.

Proof. This is easily proved by referring to the character table for A_5 . The details are left to the reader.

Henceforth we identify V^* with the space of all functions $f: S \to \mathbb{C}$ such that $\sum f(s) = 0$, as in the lemma. If f is a nonzero element of V^* , the point of $P(V^*)$ corresponding to f will be denoted by [f].

LEMMA 15. The quadric Q consists of all [f] in $\mathbf{P}(V^*)$ such that $\sum f(s)^2 = 0$, where the summation runs over all of the elements s of S.

Proof. The representation of G on V^* is irreducible, so by Schur's lemma there can be at most one invariant quadric. On the other hand, $\sum f(s)^2 = 0$ is certainly an invariant quadric. So that quadric is Q.

To go further, we need more precise information about the invariants of G in V^* . The following result is well known and follows at once from the known structure of the ring of invariants of the permutation representation of S_5 of degree 5 by reducing modulo the ideal generated by $\sum f(s)$.

LEMMA 16. For $n \ge 0$ and for all f in V^* , let

$$\alpha_n(f) = \sum f(s)^n.$$

Also let

$$D(f) = \det(d_{s,j})$$

where $(d_{s,j})$ is the $S \times 5$ matrix whose (s,j)th entry, for $s \in S$ and $0 \le j \le 4$, is given by $d_{s,j} = f(s)^j$. Then the ring of all Ginvariant polynomials on V^* is generated by α_2 , α_3 , α_4 , α_5 and

D. Furthermore, the invariants α_2 , α_3 , α_4 , α_5 form a homogeneous system of parameters for the ring of invariants and D^2 is a polynomial in α_2 , α_3 , α_4 , α_5 with integer coefficients.

The following corollary follows at once from Lemma 16.

COROLLARY. For every integer $n \ge 0$, denote by R_n the space of homogeneous invariants of degree n for G. Then we have

$$R_2 = \mathbf{C}\alpha_2,$$

$$R_3 = \mathbf{C}\alpha_3,$$

$$R_4 = \mathbf{C}\alpha_2^2 + \mathbf{C}\alpha_4,$$

$$R_5 = \mathbf{C}\alpha_2\alpha_3 + \mathbf{C}\alpha_5,$$

$$R_6 = \mathbf{C}\alpha_2^3 + \mathbf{C}\alpha_2\alpha_4 + \mathbf{C}\alpha_3^2.$$

We can now prove our results. We will identify $X(5) \times X(5)$ with the quadric Q given by $\alpha_2 = 0$ (cf. Lemma 15).

THEOREM 3. The curve Ξ on Q defined by $\alpha_2 = \alpha_3 = 0$ is a modular correspondence on X(5). In fact, if we choose the element σ appropriately, Ξ is the modular correspondence $J\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

Proof. First we will show that Ξ satisfies the hypothesis of Theorem 1 of §3. It is easy to see that Ξ is irreducible. Otherwise every component is A_5 invariant and, since Ξ has bidegree (3, 3), some component would be an A_5 -invariant rational function f from X(5)to itself of degree ≤ 2 . But then f would have ≤ 3 fixed points forming a set invariant under A_5 , which contradicts the fact that the minimal A_5 orbit has 12 points. Therefore Ξ is irreducible. If we denote by φ the automorphism of G determined by σ , we have that the stabilizer of Ξ contains the graph of φ . Also, Ξ maps any cusp to a divisor of degree 3 invariant under a cyclic subgroup of degree 5. Such a divisor must be supported on cusps. The same reasoning also applies to the transpose $\iota(\Xi)$ of Ξ . So Ξ is cuspidal. Let Λ denote the correspondence $\iota(\Xi) \circ \Xi - 3\Delta$. Then Λ has bidegree (6, 6) and therefore has 12 fixed points. This set of 12 points must be a union of G-orbits. Since the cusps of X(5) form the only orbit with ≤ 12 elements, the fixed points of Λ must all be cusps. It now follows from Corollary 1 of Lemma 12 and Theorem 1 that Ξ is a modular correspondence. Since the stabilizer of Ξ contains the graph of φ , by Lemma 6 of §4, the correspondence Ξ is of the form $J\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where

 $\binom{a\ b}{c\ d}$ has relatively prime integer entries and positive determinant prime to 5. It is convenient for us to choose σ to be the element of $S_5\cong \operatorname{PGL}_2(\mathbf{F}_5)$ represented by $\binom{2\ 0}{0\ 1}$. By Lemma 7 of §4, both $\binom{a\ b}{c\ d}$ and $\binom{2\ 0}{0\ 1}$ induce the same automorphism φ of G. So we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv t \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}.$$

By Lemma 8 of §4, we have $\psi(ad-bc)=3$, which implies that ad-bc=2. By Lemma 9 of §4, we have

$$\Xi = J\left(\eta \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

where η belongs to Γ . Therefore we have

$$\eta \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \equiv t \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}.$$

Taking determinants, we have $t \equiv \pm 1 \pmod{5}$ and therefore $\pm \eta$ belongs to $\Gamma(5)$. Therefore

$$\Xi = J \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

THEOREM 4. Let Θ be the curve on Q defined by $\alpha_2 = \alpha_4 = 0$. Then Θ is a modular correspondence of X(5). In fact, if we choose the element σ as in Theorem 1, then

$$\Theta = J\left(\eta \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

where η is any element of Γ congruent to $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ modulo 5.

Proof. Since Θ has bidegree (4, 4) and is invariant under S_5 , we have by Lemma 11 of §5 that Θ is cuspidal. Suppose that Θ_0 is an irreducible component of Θ and let (a, b) be the bidegree of Θ . Since there is no A_5 -equivariant function from X(5) to itself, neither a nor b can be 1. Therefore there can be no more than 2 components of Θ and if Θ is reducible we must have a = b = 2. Since A_5 is simple, Θ_0 must be invariant under A_5 . But then the 4 fixed points of $\iota(\Theta_0) \circ \Theta_0 - 2\Delta$ must be invariant under A_5 , which is impossible since every orbit of A_5 has at least 12 elements. Therefore Θ is irreducible. The correspondence $\iota(\Theta) \circ \Theta - 4\Delta$ has bidegree (12, 12) and commutes with the action of G on X(5). Its 24 fixed points must therefore be a union of G-orbits. Since a G-orbit on X(5) must

have order 12, 20, 30 or 60 and since the cusps form the unique 12 point orbit, the 24 fixed points must consist of the cusps taken twice. Therefore, by Corollary 1 of Lemma 12 and by Theorem 1, Θ is a modular correspondence. Letting φ be as in the proof of Theorem 3, we have by Lemma 6 of §4 that Θ is of the form $J\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has relatively prime integer entries and positive determinant prime to 5. As in Theorem 3, we suppose that σ corresponds to the element $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ of $PGL_2(\mathbf{F}_5)$. By Lemma 7 of §4, both $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ induce the same automorphism φ of G. Therefore we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv t \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}.$$

By Lemma 8 of §4, we have $\psi(ad - bc) = 4$ which implies that ad - bc = 3. By Lemma 9 of §4, we have

$$\Theta = J\left(\eta \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

where η is an element of Γ . Therefore

$$\eta \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \equiv t \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}$$

which implies that

$$\eta \equiv t \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}.$$

Taking determinants, we have $t^2 \equiv -1 \pmod{5}$. Since we are working multiplicatively modulo ± 1 anyway, we may suppose t = 3. Therefore η may be taken to be any element of Γ which is congruent to $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \pmod{5}$.

In view of the detailed understanding one has of the relevant geometry, perhaps it is possible to determine all of the modular correspondences on X(5) which arise as intersections of Q with invariant hypersurfaces.

8. The Klein curve in three dimensional space. The equation $XY^3 + YZ^3 + ZX^3 = 0$ defines a plane quatric curve $\mathscr E$ of genus 3. The curve $\mathscr E$ is invariant under a group of collineations isomorphic to $PSL_2(F_7)$. On p. 109 of [K2], Felix Klein proved that $\mathscr E$ is isomorphic to the modular curve X(7). Referring to formula (2.1) on p. 161 of W. L. Edge's paper [E1], we see that the quartic form defining $\mathscr E$ may be

expressed as a symmetric determinant, namely

$$-\frac{1}{2}(XY^{3} + YZ^{3} + ZX^{3}) = \begin{vmatrix} Y & 0 & 0 & -\tau^{-1}X \\ 0 & X & 0 & -\tau^{-1}Z \\ 0 & 0 & Z & -\tau^{-1}Y \\ -\tau^{-1}X & -\tau^{-1}Z & -\tau^{-1}Y & 0 \end{vmatrix}$$

where $\tau = \sqrt{2}$. The matrix on the right defines a quadratic form in four variables which depends linearly on X, Y and Z. Thus we have a net of quadrics in \mathbf{P}^3 . The curve $\mathscr C$ consists of those points of the plane which correspond to cones in \mathbf{P}^3 . The locus in \mathbf{P}^3 of the vertices of these cones is a twisted sextic curve K in \mathbf{P}^3 isomorphic to $\mathscr C$. The curve K is invariant under a group of collineations of \mathbf{P}^3 isomorphic to $\mathrm{PSL}_2(\mathbf{F}_7)$. Denoting by ρ and ρ' the projective representations of $\mathrm{PSL}_2(\mathbf{F}_7)$ on \mathbf{P}^2 and \mathbf{P}^3 which occur here, we have for all g in $\mathrm{PSL}_2(\mathbf{F}_7)$ that

$$\rho'(g) \cdot Q_{x} = Q_{v}$$

where $y = \rho(g) \cdot x$ and where for all t in \mathbf{P}^2 we denote by Q_t the quadric in \mathbf{P}^3 corresponding to t. In Edge's paper ([E2], §12, p. 509) it is shown that for every point p of K, the polar hyperplanes of p with respect to all of the quadrics of the net meet in a line which in turn meets K in three points. Denoting this line by $\lambda(p)$, we have that $\lambda(p)$ is a trisecant of K. Furthermore, every trisecant of K arises in this way and if p and q are points of K then p is on $\lambda(q)$ if and only if q is on $\lambda(p)$. There are three trisecants through every point of K.

Denote by G the group of collineations of \mathbf{P}^3 determined by $\mathrm{PSL}_2(\mathbf{F}_7)$. Since the operation of taking polars is covariant, it follows that for all g in G and all p in K, the trisecant $\lambda(g \cdot p)$ associated to $g \cdot p$ is the image under g of the trisecant $\lambda(p)$ associated to p. Denote by Ξ the correspondence on K which associates to each p on K the three points where $\lambda(p)$ meets K. Then the correspondence Ξ commutes with all of the collineations in G. Furthermore, since p lies on $\lambda(q)$ if and only if q lies on $\lambda(p)$, the correspondence Ξ has bidegree (3,3).

The mapping λ induces a rank 2 vector bundle on the modular curve X(7) which is invariant under the action of the group of 168 automorphisms. It would be interesting to study this bundle from the standpoint of the moduli of vector bundles on the modular curve. A similar phenomenon occurs in connection with a scroll of quadrisecants on the modular curve X(11) of level 11 (cf. [A]). In view of

the relation of both bundles to modular correspondences, it would be interesting to try to find generalizations to modular curves of higher level.

9. Identification of some modular correspondences on X(7).

Lemma 17. Every irreducible component of the correspondence Ξ is fixed by the diagonal of G and is cuspidal.

Proof. This follows at once from the corollary of Lemma 11.

LEMMA 18. Let p be a point of K. Then p does not lie on the trisecant $\lambda(p)$ associated to p.

Proof. Every orbit of G on K has at least 24 elements, so p cannot be one of the 8 base points of the net of quadrics. If p belongs to $\lambda(p)$, the point p lies on the polar plane of p with respect to each quadric Q_t of the net. But then p lies on Q_t for every t in \mathbf{P}^2 , contradicting the fact that p is not a base point of the net.

COROLLARY 1. The correspondence Ξ is an irreducible correspondence without fixed points. In particular, Ξ is cuspidal.

Proof. By Lemma 18, the correspondence Ξ has no fixed points. So it is enough to show that it is irreducible. We know that Ξ has no components of the form $\{x\} \times K$ or $K \times \{y\}$. Therefore since Ξ has bidegree (3,3), it must, if reducible, contain a correspondence T of bidegree (a,1) where $a \le 2$. Then T is the graph of a nonconstant function from the curve K to itself. Since K has genus > 1, it follows that T is the graph of an automorphism α of K. By Lemma 17, the automorphism α must lie in the center of G. Hence we have $\alpha = 1$ and T is the diagonal. But by Lemma 18, the correspondence Ξ has no fixed points. We conclude that Ξ is irreducible.

COROLLARY 2. The endomorphism of $H^1(K, \mathbb{Z})$ induced by Ξ is the identity transformation.

Proof. Denote by T the endomorphism of $H^1(K, \mathbb{Z})$ induced by Ξ . Then T commutes with the action of G on $H^1(K, \mathbb{Z})$. The group G has a representation ρ of degree 3 over $\mathbb{Q}(\sqrt{-7})$. Denote by ρ_0 the six dimensional representation of G over \mathbb{Q} obtained by viewing the representation space of ρ as a rational vector space. Then the

representation of G on $H^1(K, \mathbf{Q})$ is isomorphic to ρ_0 . Since ρ is irreducible, it follows that the endomorphism ring of $H^1(K, \mathbf{Q})$ as a G module is isomorphic to $\mathbf{Q}(\sqrt{-7})$. Therefore we can identify T with an element β of $\mathbf{Q}(\sqrt{-7})$. Since Ξ acts on $H^1(K, \mathbf{Z})$, β must in fact be an algebraic integer. On the other hand, since Ξ is symmetric, all of the eigenvalues of T in $H^1(K, \mathbf{C})$ must be real. So β is a rational integer. By Lemma 18, the correspondence Ξ has no fixed points. By the Lefschetz formula, we therefore have

$$0 = \sum_{i=1}^{2} (-1)^{i} tr(H^{i}(\Xi)) = 3 - tr(T) + 3 = 6 - 6\beta$$

since Ξ has bidegree (3, 3) and $H^1(K, \mathbb{Z})$ has rank 6. Therefore $\beta = 1$, which proves the corollary.

Theorem 5. The correspondence Ξ on X(7) is a modular correspondence. In fact, Ξ is the correspondence associated to the double coset

$$\Gamma(7)\eta\begin{pmatrix}2&0\\0&1\end{pmatrix}\Gamma(7)$$

where η is any element of Γ congruent to $\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$ modulo 7.

Proof. By Corollary 1 of Lemma 18, the correspondence Ξ is cuspidal. By Corollary 2 of Lemma 18 and the Lefschetz fixed point formula, the correspondence $\Xi \circ \Xi - 3\Delta$ has exactly 24 fixed points. Since these must be invariant under the group G, they must coincide with the set of cusps. Applying Corollary 2 of Lemma 12 of §6, we conclude that Ξ is a modular correspondence. The theorem now follows from Theorem 2 of §4.

REMARK. In view of Theorem 1, we can regard Corollary 2 of Lemma 18 as a determination of the eigenvalues of a Hecke operator acting on a space of automorphic forms using projective geometry. A more complicated example is given in [A].

Theorem 6. The correspondence Θ on K which associates to each point p of K the six points other than p where the three trisecants through p meet K is a modular correspondence. It is associated to the double coset

$$\eta^{-1}\Gamma(7)\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}\Gamma(7)$$

where η is as in Theorem 5.

Proof. We have

$$\Theta = \Xi^2 - 3\Delta,$$

where Δ is the identity correspondence of K. Clearly, Θ contains the correspondence belonging to the double coset

$$\Gamma(7)\left(\eta\begin{pmatrix}2&0\\0&1\end{pmatrix}\right)\Gamma(7)=\eta^{-1}\Gamma(7)\begin{pmatrix}4&0\\0&1\end{pmatrix}\Gamma(7)$$

which has the same bidegree (6, 6) as Θ . So Θ must equal that modular correspondence.

REMARK. Let X be a ruled surface in \mathbf{P}^3 and let Y be the double curve of X. If p is a point of Y, let $\Theta'(p)$ be the set of points, other than p, in which Y is met by generators of X passing through p. Then Θ' is a correspondence on Y. If we take X to be the ruled surface swept out by the trisecants of K, then K is the "double" curve (which is triple in this case) and the correspondence Θ' reduces to the correspondence Θ of Theorem 5. The first part of the following theorem is due to Felix Klein [K-F], p. 693). Recall that $\mathscr C$ is the plane curve defined by $XY^3 + YZ^3 + ZX^3 = 0$.

Theorem 7. Let Λ denote the correspondence on $\mathscr E$ which associates to each point p of $\mathscr E$ the six points, other than p, where $\mathscr E$ is met by the polar conic of p with respect to $\mathscr E$. Then Λ determines on X(7) the modular correspondence belonging to the double coset

$$\eta^{-1}\Gamma(7)\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}\Gamma(7)$$

where η is as in Theorem 1. In particular, Λ concides with the correspondence Θ of Theorem 6.

Proof. The correspondence Λ has bidegree (6, 6) and is symmetric, as equation (3) on page 693 of [K-F] shows. Denote by p_1 , p_2 and p_3 the points

$$p_1 = [1, 0, 0],$$

 $p_2 = [0, 1, 0],$
 $p_3 = [0, 0, 1]$

of \mathscr{C} . The polar conic of p_1 with respect to \mathscr{C} is XY=0, which cuts out the divisor $3p_1+p_2+4p_3$ on \mathscr{C} . Therefore, $\Lambda(p_1)=p_1+p_2+4p_3$. Note that p_1 , p_2 and p_3 are points of inflection of \mathscr{C} and therefore cusps of X(7). Since Ξ commutes with the elements

of G, we conclude that Ξ is cuspidal. Referring to the definition of valency given on p. 11 of [E3], we see that Λ is a correspondence of valency 2. Therefore Λ induces scalar multiplication by -2 on the cohomology group $H^1(\mathscr{C}, \mathbf{R})$. Applying the Lefschetz fixed point formula (or, what is the same in this case, the Cayley-Brill formula (cf. [E3], p. 12)) to the correspondence $\Omega = \iota(\Lambda) \circ \Lambda - 6\Delta$, we see that Ω has 72 fixed points. Since the G-orbits on \mathscr{C} have order 24, 42, 56, 84 and 168 with the only 24 point orbit being the set of cusps, and since Ω commutes with G, we see that the fixed points of Λ consist of the cusps of X(7) taken three times. We can write $\Lambda = \sum \Lambda_i$ as a sum of irreducible correspondences, where for i = 1, ..., r the correspondence Λ_i has bidegree (a_i, b_i) . Then the number r of components of Λ , counted with their multiplicities, is ≤ 6 . Since Λ is cuspidal, so is each Λ_i . Let $\Omega_i = \iota(\Lambda_i) \circ \Lambda_i - a_i \Delta$. Then Ω_i is contained in Ω , so all of the fixed points of Ω_i are cusps. By Corollary 2 of Lemma 12 of $\S 6$, each Λ_i must therefore be a modular correspondence. It then follows from Lemma 8 of §4 that $a_i = b_i$ for $1 \le i \le r$. Since the numbers 2 and 5 cannot be written in the form $\psi(D)$, Lemma 8 of §4 implies that none of the a_i can be 2 or 5. If for some i we have $a_i = 1$ then Λ_i is the graph of a function from \mathscr{C} to itself and since \mathscr{C} has genus > 1, that function must be an automorphism of \mathscr{C} . Since Λ_i is invariant under the diagonal of $G \times G$, that automorphism must lie in the center of G. Since the center of G is trivial, we conclude that if $a_i = 1$ then $\Lambda_i = \Delta$. Since $\Lambda(p_1) = p_1 + p_2 + 4p_3$, the identity correspondence Δ cannot occur more than once among the components of Λ . If Δ does occur in Λ , let $\Lambda' = \Lambda - \Delta$. Then Λ' is a symmetric correspondence of bidegree (5,5) which is invariant under G and which does not contain Δ . But that contradicts the fact that none of the a_i can equal 2 or 5. Therefore, if Λ is reducible, we must have r=2 and $a_1=a_2=3$. But then by Theorem 2 the two components Λ_1 and Λ_2 coincide, contradicting the fact that $\Lambda(p_1) = p_1 + p_2 + 4p_3$. Therefore, Λ is irreducible and we are done by Theorem 2.

REMARK. Now that we know from a transcendental point of view that the algebraic correspondences Θ of Theorem 2 and Λ of Theorem 3 coincide, it is natural to ask whether one can see how to transform one into the other using projective geometry.

¹This is in effect how one deduces the formula given in [E3], p. 12 for the number of branch points of a correspondence with valency. It is justified by Lemma 12 of §6. In general, one uses that Lemma with the Lefschetz fixed point formula.

REFERENCES

- [A] Allan Adler, Modular correspondences on X(11), to appear in Proc. Edinburgh Math. Soc.
- [E1] W. L. Edge, *The Klein group in three dimensions*, Acta Mathematica, **79** (1947), 153-223.
- [E2] _____, Octadic surfaces and plane quartic curves, Proc. London Math. Soc. (2), 43 (1937), 276-280.
- [E3] ____, The theory of ruled surfaces, Cambridge at the University Press 1931.
- [F] Ernst Wilhelm Fiedler, Ueber eine besondere Classe irrationaler Modulargleichungen der elliptischen Funktionen, Vierteljahrsschrift der Züricher Naturforschenden Gesellschaft, Bd. 30.
- [He] Otto Hesse, Über die Doppeltangenten der Curven vierter Ordnung, Crelle, Bd. 49, S. 279–332 [Ges. Werke, pp. 345–404].
- [Hu1] Adolf Hurwitz, Math. Ann., 28 (1887), 565.
- [Hu2] ____, Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip, Berichte von der kgl. Gesellschaft der Wissenschaften, mathematische-physische Klasse, (1986), 10-38; reprinted in Math. Ann., 32 (1887), 561-585 [Mathematische Werke, Band I, pp. 163-188].
- [K1] Felix Klein, Weitere Untersuchungen über Ikosaëder, Abschnitt II, §10, Math. Ann., 12 (1877), [Gesammelte Mathematische Abhandlungen, Zweiter Band, Article LIV, pp. 321-379].
- [K2] ____, Über die Transformation siebenten Ordnung der elliptischen Funktionen, Math. Ann., 14 (1878/79), 429-471 [Ges. Math. Abh., Bd. 3, pp. 90-136].
- [K-F] Felix Klein and Robert Fricke, Vorlesungen über die Theorie der elliptischen Modulfunktionen, Zweiter Band Johnson Reprint Corporation, New York/B. G. Teubner, Verlagsgesellschaft mbH, Stuttgart 1966.
- [Sh] Goro Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Kano Memorial Lectures 1, Publications of the Mathematical Society of Japan 11 Iwanami Shoten, Publishers and Princeton University Press, USA 1971.
- [Sp] Edwin H. Spanier, Algebraic Topology, McGraw-Hill Book Company, New York 1966.

Received July 31, 1990. After 1992, see CML of AMS.

36 ROLENS DRIVE APT. 4C KINGSTON, RI 02881