The Eightfold Way
MSRI Publications
Volume **35**, 1998

Invariants of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ Acting on $\mathbb{C}^n$ for $q = 2n \pm 1$

ALLAN ADLER

In fond memory of my friend and teacher Michio Kuga.

ABSTRACT. We define bicycles and present the Bicycle Conjecture, which is false in general but which we believe is neverthelesss quite useful, and derive from it specific open conjectures about some explicit conjectural generators of the bicycles of invariants of components of the Weil representation of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ and $\mathrm{Sp}_{2r}(\mathbb{F}_p)$. Construction of these generators depends on our result that the Weil representation has a unique invariant 3-tensor and our explicit computation of it, and on results on intertwining operators given in an appendix. We then give a tentative definition of the notion of "geometric construction" based on covariants. In spite of its limited scope, it is adequate for the purposes of this article. We prove that the modular curve $X(p)$ can be constructed geometrically from that 3-tensor provided p is a prime ≥ 11 and $\neq 13$. This uses our determination of the automorphism group of the invariant 3-tensor. The conjectural generators for the bicycle of invariants of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ are inspired by and generalize the generators given in the Klein–Fricke treatise for the ring of invariants of the three-dimensional representation of $\mathrm{PSL}_2(\mathbb{F}_7)$. That includes, in particular, the quartic invariant defining the Klein curve.

1. Introduction

The work described in this article was motivated by a desire to understand from a general point of view the results of Felix Klein on the equations defining modular curves of prime order, especially his remarkable discovery that the modular curve $X(11)$ is the singular locus of the Hessian of the cubic threefold

$$v^2w + w^2x + x^2y + y^2z + z^2v = 0.$$

1991 *Mathematics Subject Classification.* 15A72, 08A02, 08A40, 20C15, 20C30, 20G20, 12H05, 13N10, 13P99, 14A99, 14N99, 17D99, 20C33.

Key words and phrases. Bicycle, Galois group, hessian, invariant differential operator, pfaffian, ring of invariants, self-adjoint group, Weil representation.

This same desire has motivated much of my work over the years (see references in the bibliography), including the computation in [Adler 1981; 1992b] of the ring of invariants of a five-dimensional complex representation of $\mathrm{PSL}_2(\mathbb{F}_{11})$ and the joint work [Adler and Ramanan 1996] on moduli of abelian varieties. At the same time, these efforts have led to other problems of interest in their own right.

In this paper, we make our first attempt at a synthesis of what we have learned from our efforts. We begin in Section 2 with some general considerations about rings of invariants introduced in [Adler 1981; 1992b], specifically the concept of a *bicycle*. A bicycle is a ring equipped with an additional structure of left module over itself. The ring of invariants of a self-adjoint group of operators or, more generally, of a weakly self-adjoint group, as in Definition 2.1, is an example of a bicycle. This fact enables one to generate rings of invariants from a small number of generators using bicycle operations. After introducing the notion of a bicycle, we then state a general conjecture (2.4), called The Bicycle Conjecture, about the bicycle of invariants of a finite group. As an example in Section 2.7 shows, the conjecture is false in general. Nevertheless, we believe that it provides a powerful tool for computing rings of invariants. The papers [Adler 1981; 1992b], show how this can work.

One weakness with the Bicycle Conjecture is that it requires one to begin with some already computed invariants. Producing explicit invariants can often be quite difficult by direct computations. Therefore it is useful to know of families of representations of finite groups for which one can produce such invariants by pure thought. We begin in Section 3 with a brief discussion of the invariants of a complex three-dimensional representation of $\mathrm{SL}_2(\mathbb{F}_7)$. These were computed by Klein [1879a] and his ingenious construction of proposed generators in that case already exhibits many features of the general case. Indeed, by adapting the tricks Klein originally used, much of the work is already done for us. In Section 4, we refer to the results of [Adler 1992a; 1994], in which an explicit invariant 3-tensor Θ was constructed for the Weil representation of $\mathrm{SL}_2(\mathbb{F}_q)$, where $q = p^r$ is an odd prime power. Starting with this 3-tensor, one can construct other invariants by considering its covariants [Dieudonné and Carrell 1971; Grace and Young 1903], when it happens to be symmetric, and also by considering certain intertwining operators of the second tensor power of the Weil representation of finite symplectic groups. Thus, we have some explicit invariants and we specialize the Bicycle Conjecture to the case of these invariants. The result is then a very specific conjecture (4.2), called the Θ Conjecture, regarding the generators of the bicycle of invariants of the $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ in the component of its Weil representation of dimension $(q+\varepsilon)/2$, where ε is the quadratic character of -1 in $\mathbb{F}_q$. We do not know of any explicit invariants of $\mathrm{SL}_2(\mathbb{F}_q)$ which are not invariants of the larger group $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$.

In Section 5, we present a similar conjecture regarding the ring of invariants of the finite symplectic group $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ when -2 is a quadratic residue modulo p. In this case, we can give an explicit quartic invariant Ω for the group as well as certain invariants which we express as explicit covariants of Ω. By applying the Bicycle Conjecture to these invariants, we obtain conjectural generators (Conjecture 5.2) for the bicycle of invariants of $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ (or at least those of even degree) on the component of the Weil representation of dimension $(p+1)/2$. This conjecture is called the Ω Conjecture. From it, we can deduce other specific conjectures.

Having shown the utility of covariants in formulating explicit conjectures regarding the generators of bicycles of invariants, it is natural to ask how powerful a tool covariants provide. More precisely, given one invariant f of a finite group G, which invariants of G arise as covariants of f? Thanks to the excellent help of Gerry Schwarz (Theorem 7.1) and of David Vogan (Theorem 7.3), we have some answers to such questions and we present them in Corollary Theorem 7.5, Corollary 7.6 and Theorem 7.7.

In Section 6, we draw attention to some of the philosophical implications of questions and results of this type. More precisely, if we follow Klein in describing geometry as that which is preserved by a group action, then we have the right to ask: if that is what we mean by geometry, what do we mean by a geometric construction? For the case of classical projective geometry, we tentatively define the notion of geometric construction in terms of covariants. Very likely, ours is not the best definition and we give some criticisms of it as well in Section 6. However it does serve our purposes in this paper. These considerations also allow us to compare the geometry imposed on complex projective space by G with classical projective geometry.

As a result of the concepts introduced in Section 6 and the results of Gerry Schwarz and David Vogan mentioned above, we are able to give a qualitative generalization of the theorem of Klein about $X(11)$ mentioned in the first paragraph of this section: we prove (Theorem 7.8) that when p is a prime ≥ 11 and $\neq 13$ there *exists* a geometric construction of the modular curve $X(p)$ from the invariant 3-tensor Θ. More precisely, if -1 is a square modulo p, then one can construct Klein's A-curve of level p from the restriction of Θ to the even part of the Weil representation of $\mathrm{SL}_2(\mathbb{F}_p)$, while if -1 is not a square modulo p then one can construct Klein's z-curve from the restriction of Θ to the odd part of the Weil representation. Clearly, one cannot formulate such a theorem without asking what one means by a geometric construction.

In view of the importance of the Weil representation in our work, we include an appendix (Section 8) describing the Weil representation and the fundamental intertwining operators used in Sections 4–7. This appendix may be regarded as a sequel to [Adler 1989].

2. Group Representations and Bicycles

Let k be a field and let V be a finite-dimensional vector space over k. The k-linear functions from V to k form a vector space which we denote V^* and which we call the dual space of V. There is a natural pairing $[\,\cdot\,,\cdot\,] : V \times V^* \to k$ defined by evaluation of elements of V^* at points of V, that is, by the rule

$$[v, v^*] = v^*(v)$$

for all $v \in V$ and all $v^* \in V^*$. We will write k-linear operators on V as operators on the left and k-linear operators on V^* on the right. If α is an endomorphism of the vector space V, there is one and only one endomorphism α^* such that

$$[\alpha v, v^*] = [v, v^* \alpha^*] \tag{2.1}$$

for all $v \in V$ and all $v^* \in V^*$. Denote by $S[V]$ the symmetric algebra on V and by $S[V^*]$ the symmetric algebra on V^*. Every invertible k-linear transformation α of V extends uniquely to an automorphism of the graded k-algebra $S[V]$. We will denote that automorphism $S(\alpha)$. Similarly, we will denote by $S(\alpha^*)$ the unique extension of α^* to an automorphism of the graded k-algebra $S[V^*]$. As in the case of operators on V^*, the operator $S(\alpha^*)$ will be written on the right. If v^* is any element of V^*, the mapping $v^* : V \to k$ extends uniquely to a derivation D_v of the symmetric algebra $S[V]$. Furthermore, if α is any invertible k-linear transformation of V, the identity (2.1) implies that

$$D_{v^* \alpha^*} = D_{v^*} \circ S(\alpha). \tag{2.2}$$

Furthermore, the operators D_{v^*} with $v^* \in V^*$ commute with each other and generate the algebra, denoted $\mathcal{D}(V)$, of differential operators with constant coefficients of $S[V]$. The mapping $v^* \mapsto D_{v^*}$ extends uniquely to an isomorphism D of $S[V^*]$ onto $\mathcal{D}(V)$. The image of an element f^* of $S[V^*]$ under D will be denoted D_{f^*}. The identity (2.2) then extends to the identity

$$D_{f^* S(\alpha^*)} = D_{f^*} \circ S(\alpha).$$

Let ρ be a representation of a group G as invertible k-linear transformations on V. Then the dual representation ρ^* of G on V^* is defined by $\rho^*(g)v^* = v^* \rho(g^{-1})^*$. In particular, V^* is a left G-module with respect to ρ^*. Let σ be an automorphism of G. Then the composition $\rho \circ \sigma$ of ρ with σ is also a representation of G on V. We denote that representation by ρ^σ.

Definition 2.1. By a *weakly self-adjoint representation* we will mean a quintuple $(G, \rho, \sigma, \tau, \phi)$ where G is a group, ρ is a representation of G on a vector space V over k, σ is an automorphism of G, τ is an automorphism of k and $\phi : V \to V^*$ is a τ-semilinear isomorphism of the vector space V onto its dual space V^* such that

$$\phi(\rho^\sigma(g)v) = \rho^*(g)\phi(v) \tag{2.3}$$

for all $g \in G$ and all $v \in V$, where ρ^* denotes the dual representation of ρ and ρ^σ denotes the representation $\rho \circ \sigma$. Thus, ϕ is a τ-semilinear intertwining operator between ρ^* and ρ^σ. When it is not necessary to specify ρ, σ, τ and ϕ, we will sometimes simply speak of G as being a *weakly self-adjoint group.*

Suppose $(G,\rho,\sigma,\tau,\phi)$ is a weakly self-adjoint representation. The isomorphism ϕ extends uniquely to a τ-semilinear isomorphism $S(\phi)$ of the k-algebra $S[V]$ onto the k-algebra $S[V^*]$. The identity (2.3) then implies that

$$\phi(S(\rho^\sigma(g)f)) = S(\rho^*(g))S(\phi(f))$$

for all $f\in S[V]$. Composing the τ-semilinear algebra isomorphism $S(\phi)$ with the algebra isomorphism D, we obtain the τ-semilinear algebra isomorphism $D\circ S(\phi)$, which we will denote D^ϕ. If f,p are elements of $S[V]$ we denote by $f\#_\phi p$ the result of applying the differential operator $D^\phi(f)$ to the element p of $S[V]$. We then have

$$(S(\rho(g))f)\,\#_\phi\,(S(\rho(g))p) = S(\rho(g))(f\#_\phi p)$$

for all $f,p\in S[V]$ and all $g\in G$.

In particular, we have the following two results.

Proposition 2.2. *Let G,ρ,V,V^*,ϕ,D^ϕ be as above. Suppose that f is an element of $S[V]$ invariant under the representation ρ of G. Then $D^\phi(f)$ is a differential operator on $S[V]$ commuting with the operators $\rho(g)$ for all $g\in G$.*

Proposition 2.3. *Let G,ρ,V,V^*,ϕ,D^ϕ be as above. Suppose that f,p are elements of $S[V]$ invariant under the representation ρ of G. Then $f\#_\phi p$ is also an element of $S[V]$ invariant under the representation ρ.*

Thus, in the situation we are considering, the ring $S[V]^G$ of invariants for the representation ρ is closed under the operation $\#_\phi$. Using it, one can often represent invariant elements of $S[V]$ with considerable brevity. It also offers the advantage that from a very small number of invariants, one can generate the entire ring of invariants by means of the new operation $\#_\phi$ on invariant polynomials. For example [Adler 1981; 1992b], in the case of the group $\mathrm{PSL}_2(\mathbb{F}_{11})$ in an irreducible representation of degree 5 over the field of complex numbers, the transcendence degree of the ring of invariants over the field of complex numbers is 5 but we are able to generate it from an invariant of degree 3 and an invariant of degree 5 using ring operations and the new operation $\#_\phi$.

It therefore seems appropriate to begin the study of a new type of algebraic structure consisting of a ring R and a homomorphism from R into the ring of endomorphisms of the additive group of R. Thus, R is a ring with an exotic structure of left module over itself. That module structure is a ring homomorphism from the ring R into the ring of endomorphisms of the additive group of R. I call such a structure a *bicycle*. Therefore, we have associated a bicycle to the quintuple $(G,\rho,\sigma,\tau,\phi)$ which we will call the *bicycle of invariants* of G acting on V. This bicycle does depend on σ, τ and ϕ as well, but in practice these will be known from the context and we omit explicit mention to avoid circumlocution. In the case of the bicycle of invariants, the exotic module structure is simply D^ϕ. Hence, we may denote the bicycle of invariants by $(S[V]^G, D^\phi)$.

The category of rings is naturally embedded in the category of bicycles via the regular representations. What we have in the case of bicycles of invariants is a class of examples of of bicycles which do not arise in this way. This class has other special features which ought to be noted. First, in the bicycle of invariants of $(G, \rho, \sigma, \tau, \phi)$ the exotic module structure is an action of the ring on itself by differential operators. Thus, it is appropriate to speak of it as a *differential bicycle*.

The notion of differential bicycle is quite general, since one has a notion of differential operator on any commutative ring with unity: a differential operator of order 0 on such a ring R is just multiplication by an element of R while, for $n > 0$, an endomorphism of the additive group of R is a differential operator of order $\leq n$ if its commutator with every differential operator of order 0 is a differential operator of order $< n$. In particular, it makes sense to speak of the degree of such a differential operator as being the smallest integer n for which the operator has degree $\leq n$. This defines a filtration of the ring $\mathrm{Diff}(R)$ of differential operators on R but in general not a grading.

If the ring R happens to have a grading, one can speak of a different notion of degree for a differential operator, which we will call the *graded degree* of the operator. We will say that a differential operator $\mathcal{D}$ has graded degree n if, viewed as an endomorphism of the additive group of R, which is a graded abelian group, $\mathcal{D}$ has degree $-n$. It is not necessarily the case that a differential operator on a ring with a grading has a graded degree. Nor is it necessarily the case in general that the graded degree coincides with the degree of the differential operator in case the graded degree is well defined. If a differential operator on a graded ring is such that its graded degree is well defined and equals the degree of the differential operator, we will say that the operator has *good grades*.

If $S[V]^G$ is the ring of invariants and if we denote by M the underlying additive group of $S[V]^G$ with its exotic left module structure D^ϕ, then then we can view M as a graded module by defining the grade in M of a form of degree d to be $-d$. Hence, we introduce the concept of a *graded bicycle* by saying that a graded bicycle is a bicycle (S, Φ) such that S is a graded ring and such that whenever x and y are elements of S homogeneous of degrees m and n respectively the element $\Phi(x)(y)$ of S is homogenous of degree $n - m$. Thus the ring of invariants of a weakly self-adjoint group is a graded bicycle. Furthermore, if (S, Φ) is a graded bicycle and also a differential bicycle, we will say that (S, Φ) is a *differential graded bicycle*. We do *not* assume that for every homogeneous element x of S, the differential operator $\Phi(x)$ has good grades. The ring of invariants of a weakly self-adjoint group is a differential graded bicycle.

Although the formal definition of a bicycle as an algebraic structure is new, the practice of converting invariants into invariant differential operators goes back to roughly the middle of the 19th century. For example, in the classical study of invariants of binary forms, one in effect uses the fact that the natural representation of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}^2$ is symplectic and gives rise to a bicycle structure on the invariants of binary forms of degree n.

(Actually, the structure is richer in this case than just the bicycle structure. One has, for example, transvection operators $(f, g)^k$ for every nonnegative integer k and the bicycle operation $f\#g$ is proportional to $(f, g)^s$, where s is the degree of f.)

In the case of the ring of invariants for the simple group of order 660 in a five-dimensional irreducible representation, we have given generators and relations for the ring ([Adler 1981; 1992b]; see also Section 6 of this paper). But it would be interesting to know how to give a presentation of the *bicycle* of invariants.

In connection with the bicycle of invariants of $(G, \rho, \sigma, \tau, \phi)$, we may also consider the following rings:

(1) the ring $\mathcal{D}_1$ of differential operators generated by $S[V]^G$ and $D^\phi(S[V]^G)$;
(2) the ring $\mathcal{D}_2 = (\mathrm{Diff}(S[V]))^G$ of G invariant polynomial differential operators on V;
(3) the ring $\mathcal{D}_3 = \mathrm{Diff}(S[V]^G)$ of differential operators on $S[V]^G$;
(4) the ring $\mathcal{D}_4$ of all differential operators on the quotient field of $S[V]$ which leave $S[V]^G$ invariant modulo those that annihilate it.

It would be interesting to understand the relation among these four rings in more detail. For example, in general $\mathcal{D}_1$ is not equal to $\mathcal{D}_2$, as shown by the following counterexample ([Levasseur and Stafford 1995], after the proof of Theorem 5): one lets G be a cyclic group of order 3 acting nontrivially on $V = k = \mathbb{C}$ by multiplication by cube roots of unity. On the other hand, one does have $\mathcal{D}_1 = \mathcal{D}_2$ in case G is a Weyl group acting by reflections [Levasseur and Stafford 1995, Theorem 5; Wallach 1993]. (I am indebted to David Vogan for bringing the results of these two papers to my attention.)

In view of the ease with which the bicycle structure cuts across the lines usually drawn by algebraic independence, it is tempting to make the following conjecture:

The Bicycle Conjecture 2.4. *Let $(S[V]^G, \#^\phi)$ be the bicycle of invariants of $(G, \rho, \sigma, \tau, \phi)$. Let $P_1, \ldots, P_r$ be homogeneous elements of $S[V]^G$. Assume that the intersection of the automorphism groups of $P_1, \ldots, P_r$ is equal to G. Then every element of $S[V]^G$ can be obtained from $P_1, \ldots, P_r$ using ring operations, scalar multiplication and the new operation $\#_\phi$.*

Remark 2.5. Let m be the greatest common divisor of the degrees of $P_1, \ldots, P_r$. Let M be a multiple of m Let H denote the cartesian product of the group G and the group of M-th roots of unity. We can then extend the quintuple $(G, \rho, \sigma, \tau, \phi)$ to a quintuple $(H, \rho', \sigma', \tau, \phi)$ where ρ' sends an M-th roots of unity ξ to scalar multiplication by ξ and where σ' is the identity on M-th roots of unity. We can then apply the Bicycle Conjecture to this extended quintuple. Let $Q_1, \ldots Q_s$ be homogeneous elements of $S[V]^G$ the intersection of whose automorphism groups is H. Then every invariant of G whose degree is divisible by M is obtained from $Q_1, \ldots, Q_s$ using ring operations, scalar multiplication and the new operation

$\#_\phi$. This follows at once from the Bicycle Conjecture and from the observation that an invariant of G has degree divisible by M if and only if it is an invariant of H.

Remark 2.6. One example of the Bicycle Conjecture would be the assertion that the bicycle of invariants of the Monster in its faithful irreducible represention of lowest degree is generated by the invariant quadratic form and Griess' invariant cubic form.

Remark 2.7. It is necessary to make some requirement on the automorphism groups of the forms $P_1, \dots, P_r$. Without it, one can easily obtain counterexamples. For example, let G be the trivial group and let the set of P_i be empty. One can also take G to be the trivial group acting on a one-dimensional complex vector space, letting $r = 1$ and $P_1 = x^2$. Finally, one can take G to be any subgroup of the symmetric group S_n other than S_n itself and consider the representation of degree n of G given by permuation of the coordinates of $\mathbb{C}^n$. One can then take $P_1, \dots, P_n$ to be the elementary symmetric functions of $x_1, \dots, x_n$ and let the bicycle structure be given by

$$f\#g = f\Big(\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}\Big)g.$$

The polynomials $P_1, \dots, P_n$ are invariant under S_n and so will all polynomials derived from them by bicycle operations, so one won't get all of the invariants of G in this way.

As stated, the hypothesis of the Bicycle Conjecture is too weak. The conjecture is false for the natural permutation representation of the symmetric group S_n. Indeed, if for $k \geq 1$ we denote by α_k the sum of the k-th powers of the n variables x_i, $1 \leq i \leq n$, then the bicycle generated by α_i, α_j, with $\gcd(i, j) = 1$, $i < j$, $j > 2$, is the polynomial ring generated by all α_k with $1 \leq k \leq j$. In particular, it doesn't contain α_n if $j < n$.

One could strengthen the hypotheses by requiring that at least one or even that all of the P_i have automorphism group G. It might also be that one needs to assume the representation ρ is irreducible. One could also require that the degrees of the P_i be greater than or equal to some lower bound. Finally, whatever their degrees, one could claim only that the conjecture be true for generic choices of the P_i's. In the absence of *any* nontrivial example of a quintuple $(G, \rho, \sigma, \tau, \phi)$ for which one can prove the Bicycle Conjecture for every choice of $P_1, \dots, P_r$ satisfying even the strictest conditions we might wish to impose, it is pointless to make the conjecture more precise at this point. However, for definiteness, we will retain the version stated above throughout this paper. (It is reasonable to expect one of the variants of the conjecture mentioned here to hold and to expect that the conjectural generators we propose here for the bicycles of generators of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ do in fact generate.)

Problem 2.8. In view of the detailed knowledge we have about symmetric polynomials, and more generally about Weyl group invariants, it seems plausible that one could actually prove the Bicycle Conjecture if the polynomials P_i are chosen to have sufficiently high degree (e.g. at least one of them $> n$ in the case of S_n) and to be generic.

In order to provide further tests of the Bicycle Conjecture, in Section 4 we will present a more precise conjecture for the bicycle of invariants of the irreducible representations of degree $(q \pm 1)/2$ of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$.

3. The Tricks of Felix Klein for $\mathrm{PSL}_2(\mathbb{F}_7)$

In this section we present the generators discovered by Felix Klein for the ring of invariants of a three-dimensional complex representation of $\mathrm{PSL}_2(\mathbb{F}_7)$. Our reason for presenting this separately is that we will find that Klein's tricks, supplemented with some of our own, suffice to describe conjectural generators for $\mathrm{SL}_2(\mathbb{F}_q)$ in one component of the Weil representation in general.

The first invariant discovered by Klein is the quartic $x^3y + y^3z + z^3x$, which we will denote f in this section, following Klein. Klein was motivated to find an invariant of this degree because he knew that it would be the equation defining an embedding of the modular curve $X(7)$ of level 7 as a plane quartic curve.

The second invariant found by Klein is the Hessian of f, which he divided by a superfluous constant and denoted ∇. Explicitly,

$$\nabla = \frac{1}{54}\begin{vmatrix} \dfrac{\partial^2 f}{\partial x^2} & \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial x \partial z} \\ \dfrac{\partial^2 f}{\partial y \partial x} & \dfrac{\partial^2 f}{\partial y^2} & \dfrac{\partial^2 f}{\partial y \partial z} \\ \dfrac{\partial^2 f}{\partial z \partial x} & \dfrac{\partial^2 f}{\partial z \partial y} & \dfrac{\partial^2 f}{\partial z^2} \end{vmatrix} = 5x^2y^2z^2 - xy^5 - yz^5 - zx^5.$$

Thus, one way to get a new invariant is to compute the Hessian of a known invariant. To get the invariant C of degree 14, he bordered the Hessian matrix with the partials of the Hessian and took the determinant, dividing by a numerical factor:

$$C = \frac{1}{9}\begin{vmatrix} \dfrac{\partial^2 f}{\partial x^2} & \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial x \partial z} & \dfrac{\partial \nabla}{\partial x} \\ \dfrac{\partial^2 f}{\partial y \partial x} & \dfrac{\partial^2 f}{\partial y^2} & \dfrac{\partial^2 f}{\partial y \partial z} & \dfrac{\partial \nabla}{\partial y} \\ \dfrac{\partial^2 f}{\partial z \partial x} & \dfrac{\partial^2 f}{\partial z \partial y} & \dfrac{\partial^2 f}{\partial z^2} & \dfrac{\partial \nabla}{\partial z} \\ \dfrac{\partial \nabla}{\partial x} & \dfrac{\partial \nabla}{\partial y} & \dfrac{\partial \nabla}{\partial z} & 0 \end{vmatrix}.$$

Thus, another trick to obtain a new invariant from an old one is to border the Hessian with the first partials of the Hessian. Finally, there is Klein's trick of taking the Jacobian of the 3 algebraically independent forms f, ∇ and C to produce the invariant K of degree 21:

$$K = \text{const} \cdot \begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial \nabla}{\partial x} & \frac{\partial C}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial \nabla}{\partial y} & \frac{\partial C}{\partial y} \\ \frac{\partial f}{\partial z} & \frac{\partial \nabla}{\partial z} & \frac{\partial C}{\partial z} \end{vmatrix} .$$

Thus, one can always try to produce new invariants from old ones by taking Jacobian determinants. Note that whereas f, ∇ and C all have even degree, the invariant K has odd degree. In general, if one has n algebraically independent forms of even degree in n variables, one can take their Jacobian and obtain a nonzero form. Moreover, if n is odd, as it is in our case, the Jacobian will have odd degree. Thus, Klein's trick is also a trick to obtain an invariant of odd degree from invariants of even degree.

Part of the beauty of Klein's generators lies in the fact that they have interesting geometric interpretations. The curve $f = 0$ in $\mathbb{P}^2(\mathbb{C})$ is, as noted, the modular curve of level 7 embedded by a natural basis for its holomorphic 1-forms. The curve $\nabla = 0$ is the locus of all points in the plane whose polar conics with respect to the quartic $f = 0$ are singular. The curve $C = 0$ is the locus of all points in the plane whose polar lines with respect to the Hessian $\nabla = 0$ are tangent to their polar conics with respect to the Klein curve $f = 0$. Furthermore, the curve $C = 0$ meets the Klein curve at the points of contact of its 28 bitangents. The curve $K = 0$ is the locus of all points whose polar lines with respect to $f = 0$, $\nabla = 0$ and $C = 0$ are concurrent. It also may be described in the following way: the group $\mathrm{PSL}_2(\mathbb{F}_7)$ has 21 elements of order 2. Each such involution fixes a projective line in $\mathbb{P}^2(\mathbb{C})$ as well as a point. Thus, the 21 lines associated to the 21 involutions form a reducible curve of degree 21 invariant under the group. Since there is only one invariant curve of degree 21, it must be $K = 0$. In particular, K is the product of 21 linear factors.

Klein also knew how to write the quartic f as a 4×4 determinant whose entries are linear forms in x, y, z. This fact may be expressed by saying that one may associate to f a net of quadrics in projective space and the Klein curve is the locus of singular quadrics. The locus of the singular points of the singular quadrics is a twisted curve of degree 6 and genus 3 isomorphic to the Klein curve.

Henceforth, we will freely use the notation introduced in the Appendix (Section 8). The reader is strongly advised to read the leisurely discussion there before proceeding, if only to gain passive knowledge of the relevant notation. However, to the more adventurous readers who prefer jungles to sidewalks, we offer the list of notation below as a machete. To facilitate such an index, groups of paragraphs of Section 8 have been numbered. Some notation is listed more than once, signifying that it has been redefined, specialized or generalized. This is especially the case for the Weil representation which is defined according to [Weil 1964] in 8.9 and denoted r_Γ, adapted to the case of finite symplectic groups $\mathrm{Sp}_{2n}(\mathbb{F}_p)$ in 8.12 and denoted r', composed with automorphisms σ_ν for $\nu\in\mathbb{F}_p^\times$ in 8.16 and denoted r'_ν, allowed to act on tensor powers of the version of 8.16 in 8.18 without change of notation, restricted to the subspaces $V_\nu^+=V^+$, $V_\nu^-=V^-$ of even and odd functions in 8.21 and denoted $\rho_\nu^\pm$, restricted to the symplectic groups $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ of odd characteristic in 8.25 and denoted r'_ν with ν still a nonzero element of $\mathbb{F}_p$, and finally generalized to the case where ν is a nonzero element of $\mathbb{F}_q$ in 8.28. Derived notation such as ρ_ν^ε is not explicitly redefined in each context and the reader is expected to be able to make the necessary modifications without difficulty.

8.1	$G,\ G^*,\ \mathbb{T},\ A(G),\ \langle\,\cdot\,,\cdot\,\rangle$
8.2	$\mathbb{T}_0,\ A_0(G)$
8.3.1	$t_0(f)$
8.3.2	$d_0(\alpha)$
8.3.3	$d_0'(\gamma)$
8.4	$B(G)$
8.5	$L_2(G),\ U$
8.6	$\mathbf{A}(G),\ \mathbf{B}_0(G),\ \pi$
8.7.1	$\boldsymbol{t}_0(f)$
8.7.2	$\boldsymbol{d}_0(\alpha),\ \lvert\alpha\rvert$
8.7.3	$\boldsymbol{d}_0'(\gamma),\ \Phi^*,\ \lvert\gamma\rvert$
8.9	$B_0(G,\ \Gamma),\ r_\Gamma$
8.10	$\mathrm{Sp}(G),\ \mathrm{Sp}'(G)$
8.11	$\mathbf{B}_1(G),\ (E),\ V^+,\ V^-,\ S^+,\ S^-$
8.12	$G,\ \chi,\ \phi,\ Sp''(G),\ r'$
8.14	$G,\ \left(\frac{\cdot}{p}\right)$
8.15	$\nu,\ \sigma_\nu,\ s_\nu,\ s$
8.16	r'_ν
8.18	$r',\ r'_\nu,\ \boldsymbol{t}_0(f),\ \boldsymbol{d}_0(\alpha),\ \boldsymbol{d}_0'(\gamma)$
8.19	$\mathcal{T}$
8.21	$\rho_\nu^+,\ \rho_\nu^-,\ V_\nu^+,\ V_\nu^-$
8.24	$\mathcal{T}_{a,\,b}$
8.25	$r',\ r'_\nu$
8.26	$A^\#(G),\ [\,\cdot\,,\cdot\,],\ \mathrm{tr},\ \tau$
8.28	$\sigma_\nu,\ s_\nu,\ r'_\nu$
8.31	$\tau_a,\ \langle\,\cdot\,,\cdot\,\rangle,\ \mathcal{Q},\ \mathcal{Q}^+,\ \mathcal{Q}^-$

4. Conjectural Generators of the Bicycle of Invariants of $\mathrm{Aut}(\mathbb{F}_q) \cdot \mathrm{SL}_2(\mathbb{F}_q)$

In this section, we will try to provide a general context for the various tricks just studied. Let $q = p^r$ be an odd prime power and let ν be a nonzero element of $\mathbb{F}_q$. In [Adler 1992a; 1994] I showed (cf. 8.27–8.28) that there is a unique (up to scalar multiple) 3-tensor on $L_2(\mathbb{F}_q)$ invariant under the Weil representation r'_ν, and I wrote it down explicitly in general. We denote this 3-tensor by Θ. Let ε be the quadratic character of -1 in the finite field $\mathbb{F}_q$ and let η be the quadratic character of -2 in $\mathbb{F}_q$. Then Θ actually arises from an invariant 3-tensor on V_ν^+ if $\varepsilon = 1$ and on V_ν^- if $\varepsilon = -1$. If we abuse notation by identifying ε with its sign, we can say that Θ arises from a ρ_ν^ε-invariant 3-tensor on V_ν^ε. Further, Θ is a symmetric 3-tensor if $\eta = 1$ and is an alternating 3-tensor if $\eta = -1$. We can express this by saying that Θ is *η-symmetric*.

Regarding Θ as a 3-tensor on V_ν^ε, one can ask for the group of linear transformations of V_ν^ε which preserve Θ. In [Adler 1994], it was shown that for $q \geq 11$ the automorphism group is generated by the group

$$\rho_\nu^\varepsilon(\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q))$$

and the group of scalar multiplications by cube roots of unity, provided that $q \neq 13$. Here, $\mathrm{Aut}(\mathbb{F}_q)$ denotes the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ denotes the semidirect product of $\mathrm{Aut}(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$. If $q = 13$, then the automorphism group is the complex Lie group G_2.

We now have 4 cases, according to the value of q modulo 8; these cases will be denoted 1, 3, 5, 7.

Case 1: If q is congruent to 1 modulo 8, we have $\eta = \varepsilon = 1$. We can write q in the form

$$q = 8n + 1.$$

The dimension of V^+ is $4n + 1$ and Θ is a cubic form on V^+. On the other hand, since q is congruent to 1 modulo 4, the representation of $\mathrm{SL}_2(\mathbb{F}_q)$ on V_ν^+ is orthogonal. The invariant quadratic form $\mathcal{Q}^+$ is given explicitly at the end of the appendix. According to the Bicycle Conjecture, we expect Θ and $\mathcal{Q}^+$ to generate the bicycle of invariants.

We could also have used Klein's tricks to produce the other conjectural generators, but it is clearly better to use the invariant quadratic $\mathcal{Q}^+$ as long as it is handy. The same remark applies, *mutatis mutandis*, in the case $q = 8n + 5$ below.

Case 3: If q is congruent to 3 modulo 8, then we have $\eta = 1$, $\varepsilon = -1$ and we can write q in the form

$$q = 8n + 3.$$

The dimension of V^- is $4n + 1$ and Θ is a cubic form on V^-. The Hessian of Θ is a form of degree $4n + 1$. If 3 doesn't divide $4n + 1$ then the Bicycle Conjecture implies that the bicycle of invariants is generated by Θ and its Hessian. If 3 does divide $4n+1$ then the bordered Hessian has degree

$$(4n-1)+2(4n)=12n-1,$$

which is not divisible by 3. In this case, the Bicycle Conjecture implies that the bicycle of invariants is generated by Θ and the bordered Hessian.

At the end of this section, we will describe a way of producing an invariant of degree $(q+1)/4$ from Θ by using certain intertwining operators.

REMARK 4.1. We have tacitly assumed that neither the Hessian determinant nor the bordered Hessian determinant is zero. We will make that assumption without explicit mention in all that follows. However, it certainly needs to be checked in any test of these conjectures. In cases 5 and 7 below, we will further assume that the invariants Ψ and Ψ' have automorphism group no bigger than that of Θ. In the case where q is a prime p of the form $4m+3$, this follows from the fact [Adler 1994] that $\mathrm{PSL}_2(\mathbb{F}_p)$ is a maximal algebraic subgroup of $\mathrm{PSL}_n(\mathbb{C})$ for $n=(p\pm1)/2$. If p is congruent to 1 modulo 4 and $p\neq 13$, then the only algebraic subgroups of $\mathrm{PSL}_n(\mathbb{C})$ that could contain $\mathrm{PSL}_2(\mathbb{F}_p)$ are the orthogonal group $O(\frac{p+1}{2},\mathbb{C})$, if $\varepsilon=1$, or the symplectic group $\mathrm{Sp}(\frac{p-1}{2},\mathbb{C})$, if $\varepsilon=-1$. Of these two possibilties, only the orthogonal group has any polynomial invariants. Any homogeneous invariant for the orthogonal group is a power of the invariant quadratic form and in particular has even degree. Since the degree of Ψ is $4n+2$, it is conceivable that it is a power of the quadratic form. So we are assuming that this is not the case. However, as long as one is conjecturing, one might as well conjecture that the automorphism group is well behaved even when q is not a prime.

In the two preceding cases, we had $\eta=1$, which meant that the 3-tensor Θ was a cubic polynomial. In the remaining cases $\eta=-1$, which implies that the 3-tensor is alternating. We must therefore rely on different methods to produce invariants. However, we can still use Θ for that purpose by means of various tricks. By combining these tricks with those of Felix Klein, we can handle the remaining cases without difficulty.

Case 5: If q is congruent to 5 modulo 8, then we have $\eta=-1$ and $\varepsilon=1$ and we can write

$$q=8n+5.$$

In this case, Θ is an alternating 3-tensor on V^+. Since we will now deal with various Weil representations and we will want to keep track of them, we will say instead that it is an alternating 3-tensor on V^+_ν. We can then regard Θ as an equivariant mapping from V^+_ν to $\bigwedge^2 V^+_{-\nu}$. Since the dimension $4n+3$ of $V^+_{-\nu}$ is odd, we cannot obtain a nonzero invariant by composing with the Pfaffian. However, we can instead use the fundamental intertwining operator $\mathcal{T}$ to map $\bigwedge^2 V^+_{-\nu}$ isomorphically onto $\mathrm{Sym}^2 V^-_{-2\nu}$. Composing $\mathcal{T}\circ\Theta$ with the determinant on $\mathrm{Sym}^2 V^-_{-2\nu}$, we obtain an invariant Ψ of degree $4n+2$ on $V^- + \nu$. Since q is congruent to 1 modulo 4, we know that there is also an invariant $\mathcal{Q}^+$ of degree 2. If we assume that Ψ is nonzero and has automorphism group equal to $r'(\mathrm{SL}_2(\mathbb{F}_q)\cdot \mathrm{Aut}(\mathbb{F}_q))$ modulo scalars, then according to the Bicycle Conjecture, we can generate every invariant of even degree on V^+_ν from Ψ and $\mathcal{Q}^+$ using bicycle operations. However, there are certainly invariants of odd degree and we would like to get them too. It is enough, assuming the Bicycle Conjecture, to get just one of them. We can do that by adopting the trick used by Felix Klein to get his invariant K of degree 21 for $\mathrm{PSL}_2(\mathbb{F}_7)$, that is, by taking a Jacobian determinant. Indeed, once we have used bicycle operations to generate $4n+3$ algebraically independent forms of even degree starting with Ψ and $\mathcal{Q}^+$, we can then take their Jacobian determinant to get a form of odd degree. Using it and bicycle operations, we get the full bicycle of invariants.

We remark that the case $q = 13$ requires some additional concern since the automorphism group of Θ on V^+ is the complex Lie group G_2 in that case. However, since the construction of the proposed bicycle generators involves the use of the intertwining operator $\mathcal{T}$, which is only invariant under the smaller group $\mathrm{SL}_2(\mathbb{F}_{13})$, we don't have to worry about G_2. A similar phenomenon occurs in connection with the case $q = 7$, which will be discussed below.

The remaining case where q is congruent to 7 modulo 8 requires more care but requires no more than the 3-tensor Θ, the more general intertwining operators $\mathcal{T}_{a,b}$ and the tricks of Felix Klein. We begin by using $\mathcal{T}_{a,b}$ to produce a "twisted" version of the 3-tensor Θ. After that, we will turn to the details of Case 7.

By tensoring $\mathcal{T}_{a,b}$ with the identity operator on $L_2(G)$, we obtain an intertwining operator between

$$r'_{\nu,\nu,\nu} = r'_\nu \otimes r'_\nu \otimes r'_\nu \quad \text{and} \quad r'_{\mu,\mu,\nu} = r'_\mu \otimes r'_\mu \otimes r'_\nu,$$

where $\mu = (a^2+b^2)\nu$. We will denote this intertwining operator by $\mathcal{T}_{a,b}\otimes 1$. Using the intertwining operator $\mathcal{T}_{a,b}\otimes 1$, we can regard the invariant 3-tensor Θ as an invariant 3-tensor, denoted Θ', for the representation $r'_{\mu,\mu,\nu}$ or, what is the same, as an equivariant mapping from r'_ν to $r'_{-\mu,-\mu}$. The existence of this invariant 3-tensor can also be shown using the same proof given in [Adler 1992a, Theorem 1] for the existence of Θ; even the computation is the same, up to the order of the terms to be added. It is also possible to write the invariant 3-tensor Θ' down explicitly by suitably adapting the methods and results of [Adler 1992a]. As in that paper, we can write Θ' in the form

$$\sum \kappa(x,y,z)\delta_x \otimes \delta_y \otimes \delta_z,$$

where δ_t denotes the delta function at t for all $t \in \mathbb{F}_q$, where $\kappa(x,y,z)$ is a complex number and where the summation runs over all elements (x,y,z) of $\mathbb{F}_q^3$ By acting on Θ' with the element $r'_{\mu,\mu,\nu}$, we see that $\kappa(\mu,\mu,\nu)$ vanishes unless

$$\mu(z^2+y^2)+\nu z^2 = 0.$$

Let Q denote the space of binary quadratic forms with entries in $\mathbb{F}_q$, which we identify with their matrices. Let i, j be elements of $\mathbb{F}_q$ such that $i^2 + j^2 \neq 0$. Define the bijective linear mapping

$$\lambda : \mathbb{F}_q^3 \to Q$$

by

$$\lambda(x, y, z) = \begin{pmatrix} \nu z + ix + jy & jx - iy \\ jx - iy & \nu z - ix - jy \end{pmatrix}.$$

The determinant of $\lambda(x, y, z)$ is easily seen to be

$$\nu^2 - (i^2 + j^2)(x^2 + y^2).$$

Therefore, if we choose i, j such that $i^2 + j^2 = -\nu\mu$, we see that the coefficient $\kappa(x, y, z)$ vanishes unless the determinant of $\lambda(x, y, z)$ is zero. It follows as in [Adler 1992a] that we can take the coefficient $\kappa(x, y, z)$ to be given by

$$\kappa(x, y, z) = \begin{cases} 0 & \text{if } \lambda(x, y, z) \text{ has rank 2}, \\ 0 & \text{if } \lambda(x, y, z) = 0, \\ 1 & \text{if } \lambda(x, y, z) \text{ is the square of a linear form}, \\ -1 & \text{otherwise}. \end{cases}$$

The quadratic form $\lambda(x, y, z)$ is given by

$$(\nu z + ix + jy)s^2 + 2(jx - iy)st + (\nu z - ix - jy)t^2.$$

We cannot expect the coefficients $\kappa(x, y, z)$ to have nice properties under all permutations of x, y, z since the quadratic form $\mu(x^2 + y^2) + \nu z^2$ doesn't. But it is reasonable to expect good behavior under interchange of x, y. Indeed, we have

$$\kappa(y, x, z) = \left(\frac{-2\mu\nu}{\mathbb{F}_q}\right) \kappa(x, y, z), \tag{4.1}$$

where the coefficient of $\kappa(x, y, z)$ on the right hand side is the quadratic character of $-2\mu\nu$ in the finite field $\mathbb{F}_q$. If we take μ to be a square and ν to be a nonsquare in $\mathbb{F}_q$ then the coefficient of $\kappa(x, y, z)$ is the negative of the quadratic character of -2 in $\mathbb{F}_q$, that is, the symmetry properties of this "twisted" 3-tensor invariant under switching x, y are the *opposite* of those of the original 3-tensor Θ. As for the behavior of $\kappa(x, y, z)$ under replacing one or more of x, y, z by their negatives, we find that

$$\kappa(-x, y, z) = \kappa(x, -y, z) = -\left(\frac{-1}{\mathbb{F}_q}\right) \kappa(x, y, z) \tag{4.2}$$

and

$$\kappa(x, y, -z) = \left(\frac{-1}{\mathbb{F}_q}\right) \kappa(x, y, z). \tag{4.3}$$

We may regard the $r'_{\mu,\mu,\nu}$-invariant 3-tensor Θ' as an equivariant mapping from r'_ν to $r'_{-\mu,-\mu}$. It now follows from (4.1), (4.2) and (4.3) that Θ' gives rise to an equivariant mapping

$$V_\nu^- \to \bigotimes\nolimits_\eta^2 V_{-\mu}^+$$

if $\varepsilon = -1$ and to an equivariant mapping

$$V_\nu^+ \to \bigotimes\nolimits_\eta^2 V_{-\mu}^-$$

if $\varepsilon = 1$, where $\bigotimes_\eta^2$ is defined by

$$\bigotimes\nolimits_\eta^2 = \begin{cases} \mathrm{Sym}^2 & \text{if } \eta = -1 \\ \bigwedge^2 & \text{if } \eta = 1 \end{cases}$$

Case 7: In the case at hand, we have q congruent to 7 modulo 8. Therefore we have $\eta = \varepsilon = -1$ and we can write q in the form

$$q = 8n - 1.$$

The twisted invariant 3-tensor then gives us an equivariant mapping

$$V_\nu^- \to \mathrm{Sym}^2 V_{-\mu}^+.$$

Composing this mapping with the determinant, we obtain an invariant Ψ' of degree $4n$ on V_ν^-. In the special case $p = 7$, the invariant Ψ' is none other than Klein's quartic

$$x^3y + y^3z + z^3x,$$

up to a scalar factor. It is therefore not surprising that Klein's tricks work in this case as well to give us conjectural generators of the bicycle of invariants. Indeed, the Hessian of Ψ' has degree

$$(4n - 2)(4n - 1)$$

and the greatest common divisor of the degrees of Ψ' and of its Hessian is 2. Therefore, according to the Bicycle Conjecture, the bicycle of all invariants of even degree of $\mathrm{SL}_2(\mathbb{F}_q)$ in V_ν^- is generated by Ψ' and its Hessian. Since the space V_ν^- has odd dimension, we can also get an invariant of odd degree by using Klein's trick of taking the Jacobian determinant of $4n - 1$ algebraically independent invariants of even degree.

We note here that in the case $q = 7$, the automorphism group of Θ on V^- is $\mathrm{SL}_3(\mathbb{C})$, not $\mathrm{PSL}_2(\mathbb{F}_7)$. However, since the construction of Klein's quartic from Θ involves the use of the intertwining operator $\mathcal{T}_{a,b}$, which is not invariant under $\mathrm{SL}_3(\mathbb{C})$, we are cut down to the smaller group $\mathrm{PSL}_2(\mathbb{F}_7)$. This is similar to what happened in the case $q = 13$ with the group G_2.

THE Θ CONJECTURE 4.2. *The following table gives conjectural bicycle generators for* $\mathrm{SL}_2(\mathbb{F}_q)$ *acting on* V_ν^ε:

$q\equiv 1 \pmod 8$	Θ, $\mathcal{Q}^+$
$q\equiv 3 \pmod 8$, $\not\equiv 1 \pmod 6$	Θ, Hessian(Θ)
$q\equiv 3 \pmod 8$, $\equiv 1 \pmod 6$	Θ, Bordered Hessian(Θ)
$q\equiv 5 \pmod 8$	Ψ, $\mathcal{Q}^+$, Jacobian
$q\equiv 7 \pmod 8$	Ψ', Hessian(Ψ), Jacobian

Thus we have conjectural generators of the bicycle of invariants of $\mathrm{SL}_2(\mathbb{F}_q)$ in V^ε in every case. Unfortunately, our methods so far tell us essentially nothing about the case of the other component of the Weil representation. In the next section, we will try to improve the situation a little. We will merely close this section with two simple remarks.

REMARK 4.3. Our examination of the invariant 3-tensor Θ and the invariant "twisted" 3-tensor Θ' provides us with an essentially unique nonassociative algebra structure on $L_2(\mathbb{F}_q)$ invariant under $\mathrm{SL}_2(\mathbb{F}_q)\cdot\mathrm{Aut}(\mathbb{F}_q)$.

REMARK 4.4. Our construction of Klein's quartic from Θ shows, among other things, how to write Klein's quartic explicitly as a symmetric 4×4 determinant whose entries are linear forms on V_ν^-. Klein [1879a; 1890–92, vol. II, ch. V] gave an explicit representation of his own quartic and studied the geometry of the associated curve in projective space as well as the plane curve. This study was taken further by H. F. Baker [1935] and especially by W. L. Edge [1947], who made a detailed study of the geometry of the net of quadrics determined by Klein's determinantal representation. In view of the fact that this determinantal representation is herein generalized to the case $q=8n-1$, it appears that [Edge 1947] might be a source of considerable inspiration for what to prove in the general case. We also note that Klein's cubic form

$$v^2w+w^2x+x^2y+y^2z+z^2v,$$

which arises in our setting as the invariant 3-tensor Θ in the case $q=11$, can be expressed as the Pfaffian of an alternating 6×6 matrix whose entries are linear forms in 5 variables. Indeed, in the general case $q=8n+3$, we can regard the invariant 3-tensor Θ as an equivariant mapping from V_ν^- to $\mathrm{Sym}^2 V_{-\nu}^-$. Composing this equivariant mapping with the fundamental intertwining operator $\mathcal{T}$, we obtain an equivariant mapping from V_ν^- to $\bigwedge^2 V_{-2\nu}^+$. Composing this mapping with the Pfaffian, we obtain an invariant of degree $(q+1)/4$ on V_ν^-. In case $q=11$, that degree is 3 and we have expressed our unique cubic invariant as a Pfaffian, as promised. This Pfaffian representation therefore appears to be on an equal footing, from our general point of view, with the determinantal representation of Klein's quartic. Explicitly, Klein's cubic is the Pfaffian of the following skew-symmetric matrix:

$$\begin{pmatrix} 0 & v & w & x & y & z \\ -v & 0 & 0 & z & -x & 0 \\ -w & 0 & 0 & 0 & v & -y \\ -x & -z & 0 & 0 & 0 & w \\ -y & x & -v & 0 & 0 & 0 \\ -z & 0 & y & -w & 0 & 0 \end{pmatrix}.$$

Finally, we note that in the special case $q = 11$, every point of Klein's cubic threefold in projective 4 space $\mathbb{P}(V_\nu^-)$ determines a projective line in projective 5 space $\mathbb{P}(V_\nu^+)$ and the locus swept out by these lines is defined by the unique quartic invariant of $\mathrm{SL}_2(\mathbb{F}_{11})$ in V_ν^+. As noted in [Adler 1997], the singular locus of that quartic is birationally equivalent to the modular curve $X(11)$.

5. Conjectural Generators of the Bicycle of Invariants of $\mathrm{Sp}(\mathbb{F}_p^r)$ on V_ν^+

As in the preceding section, let p be an odd prime number and let r be a positive integer. If $p = 3$, we will assume that $r > 1$. We have the Weil representation r'_ν of $\mathrm{Sp}(\mathbb{F}_p^r)$ on $L_2(\mathbb{F}_p^r)$ and its tensor powers, which are also denoted r'_ν. According to Lemma 8.23, the canonical intertwining operator $\mathcal{T}$ maps $\mathrm{Sym}^2(V_\nu^+)$ onto $\mathrm{Sym}^2(V_{2\nu}^+)$. Since the dual space of $\mathrm{Sym}^2(V_\nu^+)$ is $\mathrm{Sym}^2(V_{-\nu}^+)$, the canonical interwining operator can be viewed as mapping $\mathrm{Sym}^2(V_\nu^+)$ onto its dual if -2 is a square modulo p. We will assume that this is the case. More precisely, we can use the intertwining operator $\mathcal{T}_{a,a}$ where a is an element of $\mathbb{F}_p$ such that $2a^2 = -1$ to map $\mathrm{Sym}^2(V_\nu^+)$ onto $\mathrm{Sym}^2(V_{-\nu}^+)$. We therefore obtain a linear form on $\mathrm{Sym}^2(V_\nu^+) \otimes \mathrm{Sym}^2(V_\nu^+)$ whose restriction to $\mathrm{Sym}^4(V_\nu^+)$ is a $\mathrm{Sp}(\mathbb{F}_p^r)$-invariant quartic form Ω on the even part of the Weil representation.

Theorem 5.1. *The quartic form Ω is nonzero.*

Proof. As in the proof of Lemma 8.23, we may regard an element of $\mathrm{Sym}^2(V_\nu^+)$ as a function $f(x, y)$ such that

$$f(-x, y) = f(x, -y) = f(y, x)$$

for all $x, y \in \mathbb{F}_p^r$. We want to show that for some $f \in \mathrm{Sym}^2(V_\nu^+)$ we have

$$\Omega(f) \neq 0$$

or, what is the same, that

$$(\mathcal{T}_{a,a} f)(f) \neq 0.$$

The linear form

$$\beta : \mathrm{Sym}^2(V_\nu^+) \otimes \mathrm{Sym}^2(V_{-\nu}^+) \to \mathbb{C}$$

given by

$$\beta(f, g) = \sum f(x, y) g(x, y),$$

where the summation runs over all $x, y \in \mathbb{F}_p^r$, is a nondegenerate pairing which is invariant under the action of

$$\mathrm{Sym}^2(\rho_\nu^+)\otimes\mathrm{Sym}^2(\rho_{-\nu}^+).$$

Therefore we only have to check that for some f in $\mathrm{Sym}^2(V_\nu^+)$ of the form $g\otimes g$ with $g\in V_\nu^+$ we have

$$\sum f(x,y)f(ax+ay,ax-ay)\neq 0,$$

where the summation runs over all $x,y\in\mathbb{F}_p$. We will take f to be the function which is 1 at $(0,0)$ and 0 elsewhere. We then have

$$\sum f(x,y)f(ax+ay,ax-ay)=1,$$

which proves that the quartic invariant is nonzero. □

We can write the quartic invariant explicitly as follows. Let $Y\in V_\nu^+$. Then the invariant is

$$\sum(Y\otimes Y)(x,y)(Y\otimes Y)(ax+ay,\ ax-ay)=\sum Y(x)Y(y)Y(ax+ay)Y(ax-ay).$$

For example, the unique quartic invariant of $\mathrm{SL}_2(\mathbb{F}_7)$ in 4 variables and of $\mathrm{SL}_2(\mathbb{F}_{11})$ in 6 variables arise in this way. For the case $p=3$ and $r=2$, the quartic invariant was discovered by Burckhardt [1893] and studied in detail by various authors, such as Baker [1935] and Coble [1917]. In [Adler and Ramanan 1996] we generalized Burckhardt's quartic to the case $p=3$ and $r>1$ and proved that it was the unique quartic invariant for this representation. In this case, the quartic can be written in the following way. For each element u of $\mathbb{F}_3^r$, introduce a variable Y_u with the provision that $Y_{-u}=Y_u$. It is the same to introduce the variable Y_0 and, for each one-dimensional $\mathbb{F}_3$ subspace λ of $\mathbb{F}_3^r$, a variable Y_λ. Then the invariant is given by

$$\sum_{u,v\in\mathbb{F}_3^r} Y_uY_vY_{u+v}Y_{u-v},$$

which can also be written as

$$Y_0^4+8Y_0\sum Y_\lambda^3+48\sum_\pi\prod_{\lambda\subset\pi}Y_\lambda,$$

where the first summation runs over all one-dimensional subspaces of the $\mathbb{F}_3$ vector space $\mathbb{F}_3^r$, the second summation runs over all two-dimensional subspaces π and where the product runs over all one-dimensional subspaces λ contained in a given two-dimensional subspace π.

The Hessian of Ω will be denoted Υ. The form Υ has degree p^r+1. If the Bicycle Conjecture could be applied in this case, we would obtain obtain the following conjecture:

The Ω Conjecture 5.2. *If p be an odd prime and let r be a positive integer. If $p = 3$ assume that $r > 1$. Let m be the greatest common divisor of* 4 *and $p^r + 1$. If p^r is congruent to* 1 *modulo* 8 *then let $M = 2$. Otherwise let $M = 4$. Then every invariant of ρ_ν^+ of degree divisible by M is obtained from Ω and Υ by bicycle operations.*

In case $(p^r + 1)/2$ is odd we can get an invariant of odd degree from a Jacobian determinant and use it to produce all invariants.

Implicit in the above conjectures is the assumption that Υ is not zero. Assuming this to be the case, one also must be certain that the forms Ω and Υ have no automorphisms in common other than those of $\mathrm{Sp}(\mathbb{F}_p^r)$, modulo scalars. That is verified in the following lemma.

Lemma 5.3. *The automorphism group of Ω is generated by $\rho_\nu^+(\mathrm{Sp}(\mathbb{F}_p^r))$ and by scalar multiplication by fourth roots of unity. Modulo scalars the group is precisely* $\mathrm{PSp}(\mathbb{F}_p^r)$.

Proof. In [Adler 1994], it is shown that the group $\mathrm{PSp}(\mathbb{F}_p^r)$ is a maximal algebraic subgroup of the group of collineations of $\mathbb{P}^N(\mathbb{C})$, where $N = (q^r \pm 1)/2$. Therefore, since Ω has degree 4, every automorphism of Ω is the product of an element of $\mathrm{Sp}(\mathbb{F}_p^r)$ and scalar multiplication by a fourth root of unity. □

The Ω Conjecture give us conjectural generators of the bicycle of invariants of even degree for $\mathrm{Sp}(\mathbb{F}_p^r)$ on V_ν^+. If p^r is congruent to 3 modulo 4 then the center of $\mathrm{Sp}(\mathbb{F}_p^r)$ acts as -1 on V_ν^+ and all invariants are necessarily of even degree. So if p^r is congruent to 3 modulo 4, these two conjectures give us conjectural generators for the full ring of invariants of ρ_ν^+.

In the special case where $r = 1$, we are dealing with the group $\mathrm{SL}_2(\mathbb{F}_p)$. If p is congruent to 3 modulo 4, the quadratic character of -1 modulo p is $\varepsilon = -1$. In this case, the methods of the preceding section give us conjectural generators of the ring of invariants (or those of even degree, at least) in V_ν^-. The methods of this section give us conjectural generators of the ring of invariants of V_ν^+ as well. Thus we have made some progress towards completing our list of conjectures. In this section, we have also opened the door to the invariants of finite symplectic groups in general in the Weil representation. It is desirable to extend the conjectures to these cases as well.

We close this section by noting some typographical and other errors in [Adler 1994]. In the statement of Lemma 7.1 on p. 2354, the group denoted $\mathrm{PSp}_m(R)$ in (1) and (1′) should be denoted $\mathrm{PSp}_{2m}(R)$. Similarly, in the statement of Theorem 7.2 on p. 2355, the group denoted $\mathrm{PSp}_m(R)\cdot A$ in (1) and (1′) should be denoted $\mathrm{PSp}_{2m}(R)\cdot A$. On the same page, in the proof of Theorem 7.2, the groups denoted $\mathrm{PSp}_m(R)$, $\mathrm{PSp}_r(\mathbb{F}_p)$, $\mathrm{PSp}_m(\mathbb{F}_R)$ and $\mathrm{Sp}_m(\mathbb{F}_R)$ should be respectively be denoted $\mathrm{PSp}_{2m}(R)$, $\mathrm{PSp}_{2r}(\mathbb{F}_p)$, $\mathrm{PSp}_{2m}(\mathbb{F}_R)$ and $\mathrm{Sp}_{2m}(\mathbb{F}_R)$. Also, the statement of Theorem 8.2 on p. 2360 and the paragraph preceding it should read:

If η is ± 1, we will say that a tensor T is **η-symmetric** if $\eta = 1$ and T is symmetric or if $\eta = -1$ and T is skew-symmetric. If $\varepsilon = \pm 1$, then by the **ε-part** of the Weil representation, we will mean the even part if $\varepsilon = 1$ and the odd part if $\varepsilon = -1$.

Theorem (8.2): *Suppose $q \geq 11$. Let ε equal the quadratic character of -1 in $\mathbb{F}_q$ and let η equal the quadratic character of -2 in $\mathbb{F}_q$. Let $n = (q+\varepsilon)/2$. Denote by Θ the unique η-symmetric 3-tensor on the ε part of the Weil representation of $\mathrm{SL}_2(\mathbb{F}_q)$. Then the group of collineations which preserve the 3-tensor is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)\cdot\mathrm{Aut}(\mathbb{F}_q)$ unless $q = 13$, in which case the group in question is $G_2(\mathbb{C})$.*

Finally, I wish to correct my comments about the work of van der Geer in [Adler 1994]. Since the appearance of that article, I have received a copy of a letter he has written in which he acknowledges my conversation with him about the quartic invariant and its explicit form. He explains that he had obtained the explicit form of the quartic invariant of $\mathrm{Sp}_{2n}(\mathbb{F}_3)$ independently at about the same time that Ramanan and I did. Accordingly, I would like to apologize for my remarks in [Adler 1994]. I hope that this apology will serve to correct the negative impressions that my comments may have caused about the character and accomplishments of a mathematician in whose work I have found so much to admire.

6. Geometric Constructions

According to Klein's Erlangen Program, geometry is the study of the properties of a set X which are preserved by the action of a group G on the set X. One important example is complex projective n-space with the group $\mathrm{PSL}_{n+1}(\mathbb{C})$ acting on it. We are familiar with this example, as it is quite standard. But suppose G is a finite group and ρ is a homomorphism from G into $\mathrm{SL}_{n+1}(\mathbb{C})$. Then G also acts on $\mathbb{P}^n(\mathbb{C})$ and gives rise to a different notion of geometry on the same set. It is quite instructive to try to articulate the difference between these two geometries.

In these examples, we can already see that the definition of geometry given above leaves certain important details unspecified. For example, in complex projective n-space, one can spend all one's time looking only at linear subspaces. Or, one can be an algebraic geometer and consider all algebraic loci in complex projective n-space. In either case, one has the same group acting but one is really considering two different kinds of geometry. Thus, we have left unspecified the kinds of objects one might want to focus on. In practice there will be various types of objects one studies in the geometry. For example, in the projective plane, one can study points, lines, triangles, conics and so forth.

Suppose G is a group acting on a set X and suppose that we have agreed on the types of objects we will consider in this geometry. If T is a type of object, we will denote by $T(X)$ the set of all objects of type T in X. Then G acts on the set $T(X)$. Suppose T_1 and T_2 are two types of object. By a *construction* of objects of type T_2 from objects of type T_1, we mean a G-equivariant mapping from $T_1(X)$ to $T_2(X)$.

Here we have to be careful, since in practice one has certain preferences as to what kind of mappings one will allow. For example, in the case of algebraic geometry in complex projective space, we would perhaps only allow polynomial mappings or rational mappings. So in our definition of a geometric construction, we really mean to assume that we are dealing with a certain category of mappings.

I would like to examine this notion of a construction more closely in the case of complex projective space. For definiteness and for simplicity, I want to focus on the question of constructing one hypersurface from another one. If d is a positive integer and V is a complex vector space, we will denote by $S_d(V)$ the vector space of forms of degree d on V. The set of hypersurfaces of degree d in the projective space $\mathbb{P}(V)$ of lines in V may then be roughly identified with the projective space $\mathbb{P}(S_d(V))$. I say roughly because a hypersurface does not uniquely determine the form which defines it, at least if we regard the matter set theoretically. For example, in $\mathbb{P}^2$, with homogeneous coordinates x, y, z, the forms x^3y and xy^3 define the same hypersurface but are not proportional. However, I am going to overlook this difficulty and pretend that the set of hypersurfaces of degree d in $\mathbb{P}^n$ is $\mathbb{P}(S_d(V))$. The difficulty disappears if one regards a hypersurface as a scheme instead of as a set, but I want to keep the discussion elementary.

Let d, e be positive integers and suppose that

$$F : \mathbb{P}(S_d(\mathbb{C}^{n+1})) \to \mathbb{P}(S_e(\mathbb{C}^{n+1}))$$

is a geometrical construction of hypersurfaces of degree e from hypersurfaces of degree d. Since we are doing algebraic geometry, that means we want the mapping F to be a rational mapping or a polynomial mapping. One problem with using rational mappings is that if one wishes to take the result of the construction F and apply another construction to it, say F', the result may not be defined. So geometric constructions don't really give us a category. On the other hand, by writing F out explicitly in terms of the coefficients of the general form of degree d and clearing denominators, we obtain a polynomial mapping

$$\tilde{F} : S_d(\mathbb{C}^{n+1}) \to S_e(\mathbb{C}^{n+1})$$

which lifts F. Since F is by definition equivariant for the action of $\mathrm{SL}_{n+1}(\mathbb{C})$, it follows that $\tilde{F}$ is a homogeneous mapping equivariant for the action of $\mathrm{SL}_{n+1}(\mathbb{C})$. In other words, $\tilde{F}$ is precisely what one classically called a *covariant*. More generally, if W is any representation space for $\mathrm{SL}_{n+1}(\mathbb{C})$, a homogeneous polynomial mapping from W to $S_e(\mathbb{C}^{n+1})$ equivariant for $\mathrm{SL}_{n+1}(\mathbb{C})$ would be called a covariant of degree e on W. The degree of the mapping is called the *order* of the covariant. In the special case where $e = 0$, a covariant is called an *invariant*.

We should also note that by using covariants, the difficulties of composing geometric constructions disappears: one can always compose polynomials.

Classically, one also considered loci as being defined by their families of tangent hyperplanes. Since a hyperplane is a point of the dual projective space, this approach amounts to a study of loci in the dual projective space. Asking for geometric constructions of these loci amounts to asking for equivariant mappings

$$S_d(\mathbb{C}^{n+1}) \to S_e(\mathbb{C}^{n+1^*}).$$

Such a mapping is called a *contravariant.* Finally, one classically considered relations between projective space and its dual which depend geometrically on a given hypersurface. This leads one to study equivariant mappings

$$S_d(\mathbb{C}^{n+1}) \to S_e(\mathbb{C}^{n+1}) \otimes S_f(\mathbb{C}^{n+1^*}),$$

which are called *mixed concomitants.*

Now that we understand a little better what we mean by a construction in classical projective algebraic geometry, let us examine the geometry imposed on $\mathbb{P}^n$ by a representation

$$\rho : G \to \mathrm{SL}_{n+1}(\mathbb{C})$$

of a finite group G. People who studied this kind of geometry were concerned not with all loci but only with loci invariant under the action of G. The reason this was not done in the case of classical projective geometry is that the group $\mathrm{SL}_{n+1}(\mathbb{C})$ acts transitively on $\mathbb{P}^n$ and there are no invariant loci. But with the finite group G, such loci exist in abundance and geometers have long delighted in studying them.

Suppose T_1, T_2 are types of objects in this geometry. A geometric construction of objects of type T_2 from objects of type T_1 is then a G-equivariant mapping

$$T_1(\mathbb{P}^n) \to T_2(\mathbb{P}^n).$$

As before, we need to specify the category of mappings we are using and again we will side with the algebraic geometers in choosing rational or polynomial maps. But more important is the following observation: since we are only interested in invariant loci, the group G acts trivially on $T_1(\mathbb{P}^n)$ and $T_2(\mathbb{P}^n)$. Therefore *every* mapping is equivariant. The notion of a geometric construction apparently loses all of its content. To put the matter bluntly, it is as easy to do geometric constructions in this geometry as it is to write poetry in Pig Latin. (Good poetry is, of course, another matter.)

While this conclusion is at first rather disconcerting, we may take heart in the observation that herein lies one of the ways we can articulate the difference between the geometry imposed by G and classical projective algebraic geometry. Indeed, we may ask: when can a geometric construction in the G-geometry be effected by means of a construction in classical projective algebraic geometry?

For example, recall Klein's generators of the ring of invariants of $\mathrm{PSL}_2(\mathbb{F}_7)$ in a three-dimensional complex representation, which we discussed in Section 3. Klein started with the invariant quartic

$$f = x^3y + y^3z + z^3x$$

and then wrote down 3 other invariants ∇, C, K of degrees 6, 14, 21 explicitly. According to the geometry imposed on $\mathbb{P}^2$ by $\mathrm{PSL}_2(\mathbb{F}_7)$, the mere juxtaposition of f and C, for example, amounts to a geometric construction of C from f. We explore the difference between $\mathrm{PSL}_2(\mathbb{F}_7)$ geometry and classical plane projective geometry when we ask whether there is a covariant

$$S_4(\mathbb{C}^3) \to S_{14}(\mathbb{C}^3)$$

mapping f to C. And in fact, there is: Klein himself gave it when he expressed C as a constant times the 4×4 matrix obtained by bordering the matrix of second partials of f with the first partials of the Hessian ∇ of f.

Thus, one way of exploring the difference between these two geometries is to ask whether every invariant of $\mathrm{PSL}_2(\mathbb{F}_7)$ arises by applying a covariant to f. Since all of Klein's generators are given explicitly by covariants, it appears that the answer to this question is affirmative.

For another example, consider the cubic form

$$f_3 = v^2w + w^2x + x^2y + y^2z + z^2v,$$

also discovered by Klein [1879b]. It is the unique (up to constant multiple) cubic invariant of a five-dimensional irreducible complex representation of $\mathrm{SL}_2(\mathbb{F}_{11})$. I computed the generators and relations of the ring of invariants of this representation and found that it is generated by 10 polynomials

$$f_3, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}, f_{12}, f_{14},$$

where f_n has degree n. I was able to express all of the invariants explicitly using covariants of f_3 except for f_{11}. For years, I didn't know whether it was expressible by covariants or not. But as we will see in Corollary 7.6 below, it is in fact expressible in this way, as are all of the invariants.

If we write down the matrix of second partial derivatives of Klein's cubic we find that up to a trivial factor of 2, it is

$$\begin{pmatrix} w & v & 0 & 0 & z \\ v & x & w & 0 & 0 \\ 0 & w & y & x & 0 \\ 0 & 0 & x & z & y \\ z & 0 & 0 & y & v \end{pmatrix}.$$

Its determinant is the invariant I have denoted f_5 and is the Hessian of f_3 up to a factor of 32.

Now consider the locus of all point $[v, w, x, y, z]$ in $\mathbb{P}^4$ for which this matrix has rank equal to 3. Saying that the rank is at most 3 amounts to writing down the 4×4 minors of the matrix and setting them to 0. That gives us a lot of quartics which define an algebraic locus in $\mathbb{P}^4$. On the other hand, it is not difficult to show, as Klein did, that there are no points $[v, w, x, y, z]$ for which the rank is less than 3. Therefore the rank 3 locus is an algebraic locus.

Felix Klein discovered the remarkable theorem that this locus is isomorphic to the modular curve $X(11)$ of level 11. Let me call this Theorem K. He also expressed this result by saying that $X(11)$ is isomorphic to the singular locus of the hypersurface $f_5 = 0$, that is, that $X(11)$ is the singular locus of the Hessian of the cubic $f_3 = 0$. Let me call this Theorem K$'$. I would like to mention that these two theorems do not say exactly the same thing, although it is not hard to show (as Klein did) that they are really equivalent. Meanwhile let me merely note that from Theorem K$'$, it is immediately apparently how the group $\mathrm{PSL}_2(\mathbb{F}_{11})$ acts on the modular curve $X(11)$. For f_3 is an invariant of $\mathrm{PSL}_2(\mathbb{F}_{11})$, its Hessian is likewise an invariant and therefore the singular locus of the Hessian is invariant under the group.

However one states the theorem, I have always found this to be an inspiring result. One naturally wonders whether one can generalize it. This problem has occupied me for a number of years.

Actually, Klein himself found a beautiful generalization of his theorem. Let $p \geq 5$ be a prime number. Denote by $L^2(\mathbb{F}_p)$ the p-dimensional complex vector space of all (square-integrable) complex valued functions on $\mathbb{F}_p$ with respect to counting measure, that is, all functions from $\mathbb{F}_p$ to the complex numbers. We can decompose $L^2(\mathbb{F}_p)$ as the direct sum of the space V^+ of even functions and the space V^- of odd functions. The space V^- has dimension $(p-1)/2$ and its associated projective space $\mathbb{P}(V^-)$ has dimension $(p-3)/2$. If f is a nonzero element of V^-, we will denote by $[f]$ the corresponding element of $\mathbb{P}(V^-)$, in keeping with the classical notation for homogeneous coordinates.

Klein discovered the following general result:

Theorem 6.1. *The modular curve $X(p)$ is isomorphic to the locus of all $[f]$ in $\mathbb{P}(V^-)$ which for all w, x, y, z in $\mathbb{F}_p$ satisfy the identities*

$$\begin{aligned} 0 = {} & f(w+x)f(w-x)f(y+z)f(y-z) \\ & + f(w+y)f(w-y)f(z+x)f(z-x) \\ & + f(w+z)f(w-z)f(x+y)f(x-y). \end{aligned}$$

Thus, $X(p)$ is defined by a collection of quartics which we can write down explicitly. In the special case $p = 11$, we recover Klein's theorem about $X(11)$. In the case $p = 7$, we obtain the defining equation of the Klein curve,

$$x^3y + y^3z + z^3x = 0$$

As much as we may admire this theorem, it is natural to feel somewhat daunted by it. For even though we know the equations, there are an awful lot of equations and it isn't clear that they really do us any good. To persuade you otherwise, let me mention that in [Adler and Ramanan 1996, § 19] we looked closely at these equations and found that they have a simple geometric interpretation: they say that the modular curve $X(p)$ is the intersection of a Grassmannian and a 2-uply embedded projective space!

More precisely, consider the Weil representation of $\mathrm{SL}_2(\mathbb{F}_p)$ on $L_2(\mathbb{F}_p)$. Tensor this representation with itself and identify $L_2(\mathbb{F}_p) \otimes L_2(\mathbb{F}_p)$ with $L_2(\mathbb{F}_p^2)$. Define the operator T from $L_2(\mathbb{F}_p^2)$ to itself by

$$(T\Phi)(x, y) = \Phi\Big(\frac{x+y}{2}, \frac{x-y}{2}\Big).$$

Then one can show that T normalizes $\mathrm{SL}_2(\mathbb{F}_p)$ as a group of operators on $L_2(\mathbb{F}_p^2)$ and maps $\bigwedge^2(V^+)$ isomorphically onto $\mathrm{Sym}^2(V^-)$. Passing to projective spaces, we can use T to identify $\mathbb{P}(\bigwedge^2(V^+))$ with $\mathbb{P}(\mathrm{Sym}^2(V^-))$. Now, in $\mathbb{P}(\bigwedge^2(V^+))$ we have the Grassmannian Gr of complex 2-planes in V^+ and in $\mathbb{P}(\mathrm{Sym}^2(V^-))$ we have the image Ver of $\mathbb{P}(V^-)$ under the 2-uple embedding. Klein's equations say precisely that $X(p)$ is the intersection of Gr and Ver.

Incidentally, one immediate consequence of this interpretation is the otherwise non-obvious result that the modular curve $X(p)$ has a canonical $\mathrm{SL}_2(\mathbb{F}_p)$ invariant rank 2 vector bundle that it gets from the Grassmannian Gr. This vector bundle is considered in more detail in [Adler and Ramanan 1996, § 24].

If Klein already generalized his theorem about $X(11)$ (that is, Theorem K) to all p, why am I not satisfied? Well, look again at Theorem K′. It says that the modular curve $X(11)$ is the singular locus of the Hessian of $f_3 = 0$. In particular, it says that we can construct the modular curve $X(11)$ from the cubic invariant f_3. Now there is nothing in Klein's general theorem on $X(p)$ about any cubic. It just gives a bunch of quartic equations that define $X(p)$. On the other hand, Ramanan and I proved that whenever $p > 3$ is a prime congruent to 3 modulo 8 (e.g. the prime $p = 11$), there is a unique cubic invariant for the representation of $\mathrm{SL}_2(\mathbb{F}_p)$ on V^-. At least for such p, we have an invariant cubic hypersurface in $\mathbb{P}(V^-)$ and we have the modular curve $X(p)$. So we have the right to ask: can we construct the modular curve $X(p)$ geometrically from the cubic hypersurface for all such p?

More generally, for any $p > 3$ there is a unique 3-tensor Θ on $L_2(\mathbb{F}_p)$ invariant under the Weil representation of $\mathrm{SL}_2(\mathbb{F}_p)$, as we mentioned in Section 4. Thus, with essentially no restriction on p, we can ask: is there a way to construct the modular curve $X(p)$ geometrically from the invariant 3-tensor Θ? We will answer this question in the affirmative.

Suppose that instead of wanting to construct one hypersurface from another, we want to construct an invariant algebraic locus L in $\mathbb{P}^n$ from an invariant hypersurface $f = 0$, where f is an invariant. Here, the ambient geometry is supposed to be defined by a representation ρ of a finite group G. Since the invariants of ρ separate orbits of G, the algebraic locus L is the intersection of all of the invariant hypersurfaces containing it. Therefore, we can find a finite number of homogeneous invariants $I_1, \ldots, I_s$ which define the locus L set theoretically. If we can show that each of the invariants I_j is obtained from a covariant of f, then we can feel safe in asserting that the locus L can be constructed geometrically (in the set theoretic sense) from $f = 0$. This motivates the following definition.

Definition 6.2. Let $H : f = 0$ be a hypersurface in a projective space $P^d(\mathbb{C})$ of dimension d and let Z be a subvariety of $P^d(\mathbb{C})$. We say that Z *can be constructed geometrically from* H if the ideal defining Z is generated by covariants of f. We say that Z *can be constructed geometrically from* H *in the set theoretic sense* if Z is the set theoretic intersection of covariants of f.

From a theoretical point of view, the notion of geometric constructibility we are using is much too restrictive. If X is a G invariant hypersurface, it requires the locus to be an intersection of G-invariant hypersurfaces. While this may be true set theoretically, contemporary algebraic geometry requires us to consider the locus from a scheme theoretic point of view and it is certainly not reasonable to require the ideal defining Z to be generated by invariants. For example, if we take Z to be the singular locus of X, the ideal defining Z will be generated by the first partial derivatives of the form f defining X. Even if f is an invariant of G, the first partials of f in general will not be. Thus, passing to the singular locus of something geometrically constructible is not geometrical according to the definition we used. We could try to expand the notion by throwing in the singular locus construction, but that is arbitrary. It would be better to have a philosophical and comprehensive notion which is at the same time practical. Meanwhile, in the absence of one, I will leave things as they stand for the moment. It is rather like confining oneself to straightedge and compass constructions even though one cannot use them to trisect angles.

A second objection is that it our definition only addresses the question of constructing Z from a hypersurface X. It says nothing about constructing Z from some other locus W.

Remark 6.3. In Definition 6.2, there is no reason to confine ourselves to hypersurfaces except to preserve the geometric language. We could just as well speak of Z as being constructed from f. Since a polynomial is simply a symmetric tensor and the symmetric tensors form an irreducible representation of $\mathrm{SL}_{d+1}(\mathbb{C})$, we could instead take any irreducible representation of $\mathrm{SL}_{d+1}(\mathbb{C})$ on a finite-dimensional vector space W and choose an element Ξ of W. We can then consider covariants of Ξ and modify Definition 6.2 to speak of a subvariety Z of $\mathbb{P}^d$ being constructed geometrically from Ξ. We will use this more general definition in Theorem 7.7 below in the cases where -2 is not a square in $\mathbb{F}_q$.

7. Applications of Contemporary Invariant Theory

From the notion of geometric construction we are using, we see that it involves the notion of being able to extend mappings equivariant for one group to mappings equivariant for a larger group. Fortunately, contemporary invariant theory has been concerned with such questions.

We begin with a simple result whose statement and proof were kindly communicated to me by Gerry Schwarz.

THEOREM 7.1. *Let k be an algebraically closed field of characteristic zero. Let $\mathcal{G}$ be a reductive algebraic group and let V and W be representation spaces for $\mathcal{G}$ over k. Let x be a point of V such that the orbit $\mathcal{G} \cdot x$ of x under $\mathcal{G}$ is closed in V and let y be a point of W. Let $\mathcal{G}_x$ and $\mathcal{G}_y$ be the subgroups of $\mathcal{G}$ fixing x and y respectively. Then the following conditions are equivalent*:

(1) $\mathcal{G}_x \subseteq \mathcal{G}_y$;
(2) *there is a $\mathcal{G}$ equivariant polynomial mapping $\Gamma : V \to W$ such that $\Gamma(x) = y$.*

PROOF. The necessity of the condition is obvious. We prove the sufficiency. Since $\mathcal{G}_x \subseteq \mathcal{G}_y$, the map sending an element g of $\mathcal{G}$ to the element $g \cdot y$ of W factors through $\mathcal{G}/\mathcal{G}_x$. Since $X = \mathcal{G} \cdot x$ is closed in V, we may interpret the map as a $\mathcal{G}$-equivariant map f of X to W which sends x to y. The map extends to a morphism F of V to W. If N is sufficiently large, the space P of polynomial maps of degree $\leq N$ from V to W contains F and restriction to X maps P linearly and $\mathcal{G}$-equivariantly onto a space Q of maps from X to W containing f. Since $\mathcal{G}$ fixes f and since $\mathcal{G}$ is reductive, it follows that we can find an element of P which restricts to f and which is invariant under $\mathcal{G}$. □

REMARK 7.2. If $x = 0$ then the constant mapping with value y from V to W is homogeneous (of degree 0, if $y \neq 0$). If $y = 0$, then again the constant mapping with value y works. However, Theorem 7.1 does not let us conclude in general that we can find a *homogeneous* polynomial mapping Γ of V to W such that $\Gamma(x) = y$. The following counterexample is due to David Vogan. Let $\mathcal{G}$ be the a group of order 2, let V be the complex numbers $\mathbb{C}$ with $\mathcal{G}$ acting by ± 1 (that is, the non-trivial one-dimensional representation) and let W be $\mathbb{C}^2$ with the nontrivial element of $\mathcal{G}$ acting by interchange of coordinates (that is, the regular representation). Let $x = 1$ and let $y = (a, b)$, where $a \neq \pm b$. Then $\mathcal{G}_x = \mathcal{G}_y$ has order 1, so by Theorem 7.1, we can find a $\mathcal{G}$ equivariant mapping Γ from V to W carrying x to y. Suppose Γ is homogeneous. Then Γ must be of the form

$$\Gamma(z) = (az^m, bz^m)$$

for some nonnegative integer m. As z runs over all complex numbers, so does z^m, so the image of Γ will be the line in W generated by (a, b). Since V is invarant under $\mathcal{G}$, that line must be also. However, there are only two invariant lines in W and our hypothesis $a \neq \pm b$ implies that (a, b) doesn't lie on either of them.

That proves that Γ cannot be homogeneous. Close examination of this example leads to the additional condition that must be satisfied in order to guarantee the existence of a homogeneous mapping. This result, due to Dave Vogan, will be presented in Theorem 7.3 below. The proof given is also due to Vogan.

THEOREM 7.3 (VOGAN). *Let $\mathcal{G}, V, W, x, y$ be as in Theorem 7.1 and assume that x, y are both nonzero. Then the mapping Γ of Theorem 7.1 can be taken to be homogeneous if and only if the stabilizer $\mathcal{G}_{\mathbb{C}x}$ of the line $\mathbb{C}x$ through x is contained in the stabilizer $\mathcal{G}_{\mathbb{C}y}$ of the line $\mathbb{C}y$ through y.*

PROOF. Suppose that Γ is a $\mathcal{G}$ equivariant homogeneous mapping from V to W such that $\Gamma(x) = y$, say, homogeneous of degree m. Let z be a complex variable. As z runs over all complex numbers, so does z^m. Since $\Gamma(zx) = z^m y$, we conclude that the line through x is mapped by Γ onto the line through y. Since Γ is equivariant, if $g \in \mathcal{G}$ leaves the line through x invariant, it therefore must also leave the line through y invariant. This proves the necessity.

Next we assume the condition and prove its sufficiency. The group $\mathcal{G}_x$ is a normal subgroup of the group $\mathcal{G}_{\mathbb{C}x}$ and we denote the factor group by Z_x. We may identify the group Z_x with the multiplicative group of all nonzero complex numbers z such that zx lies in the orbit $\mathcal{G} \cdot x$ of x under $\mathcal{G}$. Similarly, we define the group Z_y. Both of the groups Z_x and Z_y are Zariski closed in the multiplicative group of $\mathbb{C}$. In particular, Z_x is either the whole multiplicative group or else it is a finite cyclic group. But it cannot be all of $\mathbb{C}^\times$ since we have assumed that the orbit of x is closed. Therefore the group Z_x is finite, say, of order m. Let ζ_m be a primitive m-th root of unity and let $g \in \mathcal{G}_{\mathbb{C}x}$ be such that $gx = \zeta_m x$. By hypothesis, $g \cdot y$ is a multiple of y, say λy. Since g^m fixes x, it must also fix y, so $\lambda^m = 1$. Therefore, $\lambda = \zeta_m^d$ for some integer d which is determined modulo m. It follows that any equivariant polynomial from V to W carrying x to y must be a sum of homogenous terms of degrees congruent to d modulo m. We can identify the affine coordinate ring of $\mathbb{C}x$ with the polynomial ring $\mathbb{C}[z]$ by means of the isomorphism $z \mapsto zx$ of $\mathbb{C}$ onto $\mathbb{C}x$. Denote by R_x the restriction to $\mathbb{C}x$ of the ring of invariants of $\mathcal{G}$, identified with a subring of $\mathbb{C}[z]$. Then R_x is generated by certain powers z^{rm} of z^m. By hypothesis, the orbit $\mathcal{G} \cdot x$ is closed. Since the group $\mathcal{G}$ is reductive, the invariants separate closed orbits. Therefore, the greatest common divisor of the integers rm is m. Since R_x is a ring, it must therefore contain z^{rm} for all sufficiently large values of r. In other words, for all sufficiently large r, there is an invariant j_r of degree rm such that $j_r(x) = 1$. Now let Γ be as in Theorem 7.1 and write Γ as a sum of its homogeneous parts:

$$\Gamma = \sum_{s=1}^{k} \Gamma_{d+r_s m},$$

where Γ_i denotes a homogeneous polynomial of degree i. Each of the Γ_i is of course $\mathcal{G}$ equivariant. Now choose r to be a sufficiently large integer and let

$$\Gamma' = \sum_{s=1}^{k} j_{r-r_s} \Gamma_{d+r_s m}.$$

Then Γ' is equivariant, homogeneous of degree $d + rm$ and carries x to y. This proves the sufficiency. □

In order to apply Theorems 7.1 and 7.3, we need to have simple criteria for an orbit to be closed. The following theorem of Luna provides such a criterion.

THEOREM 7.4 [Luna 1975, p. 231]. *Let k be an algebraically closed field of characteristic 0. Let $\mathcal{G}$ be a reductive algebraic group over k and let $\mathcal{H}$ be a reductive subgroup of $\mathcal{G}$, not necessarily connected. Let $N_{\mathcal{G}}(H)$ denote the normalizer of $\mathcal{H}$ in $\mathcal{G}$. Then the following two conditions are equivalent*:

(1) *the group $N_{\mathcal{G}}(\mathcal{H})/\mathcal{H}$ is finite*;
(2) *in every rational representation of finite dimension $\mathcal{G} \to GL(M)$, the $\mathcal{G}$-orbit of any fixed point of $\mathcal{H}$ in M is closed in M.*

If r, s are nonnegative integers and M is a complex vector space, denote by $\bigotimes^{r,s} M$ the tensor product $M^{\otimes r} \otimes (M^*)^{\otimes s}$ viewed as a $GL(M)$ module. If $\mathcal{G}$ is a subgroup $GL(M)$, we call a $\mathcal{G}$ submodule of $\bigotimes^{r,s} M$ an (r, s) tensor module of $\mathcal{G}$. We will call a $\mathcal{G}$ module a *tensor module* if it is isomorphic to an (r, s) tensor module of $\mathcal{G}$ for some (r, s). An element of $\bigotimes^{r,s} M$ is called a *mixed tensor* of type (r, s) of M.

THEOREM 7.5. *Let G be a reductive algebraic group and let $\rho : G \to \mathrm{SL}(M)$ be a unimodular representation of G on a finite-dimensional complex vector space. Assume that $\rho(G)$ has finite index in its normalizer in $\mathrm{SL}(M)$. (This will be the case, e.g., if $\rho(G)$ is a maximal algebraic subgroup of $\mathrm{SL}(M)$ modulo scalars.) Let T_1, T_2 be mixed tensors on M, with T_1 of type (r, s) and T_2 of type (u, v). Assume that the isotropy group of T_2 in $\mathrm{SL}(M)$ contains G and that the isotropy group of T_1 in $\mathrm{SL}(M)$ coincides with $\rho(G)$ modulo scalars and is not all of $\mathrm{SL}(M)$. Then the following two conditions are equivalent*:

(1) *There exists a homogeneous $\mathrm{SL}(M)$-equivariant polynomial $\Gamma : \bigotimes^{r,s} M \to \bigotimes^{u,v} M$ such that $\Gamma(T_1) = T_2$.*
(2) *$u - v$ is a multiple of $\gcd(r-s, m)$, where m is the dimension of M.*

PROOF. If we take $\mathcal{G} = \mathrm{SL}(M)$ and $\mathcal{H} = \rho(G)$ in Luna's Theorem, the assumption on the normalizer of $\mathcal{H}$ implies that the $\mathrm{SL}(M)$ orbit of T_1 is closed in $\bigotimes^{r,s} M$. Next, we let $\mathcal{G} = \mathrm{SL}(M)$, $V = \bigotimes^{r,s} M$, $W = \bigotimes^{u,v} M$, $x = T_1$, $y = T_2$ in Theorems 7.1 and 7.3 and consider the hypotheses of these theorems. If $\mathcal{G}_x \subseteq \mathcal{G}_y$, our assumptions on the isotropy groups of T_1 and T_2 imply that $\mathcal{G}_{\mathbb{C}x} \subseteq \mathcal{G}_{\mathbb{C}y}$. This shows that if $\mathcal{G}, V, W, x, y$ satisfy the conditions of Theorem 7.1, they also satisfy the additional condition of Theorem 7.3 and that the $\mathcal{G}$ equivariant polynomial mapping Γ can therefore be taken to be homogeneous. Since $\rho(G) \subseteq \mathcal{G}_y$, the condition that $\mathcal{G}_x \subseteq \mathcal{G}_y$ is equivalent to the condition that every scalar in $\mathcal{G}_x$ lies in $\mathcal{G}_y$. Let z be a scalar multiplication in $\mathrm{SL}(M)$. Then z is an m-th root of unity, where m is the dimension of M. Under the action of z on V (or W), the tensor x (or y) is multiplied by z^{r-s} (or z^{u-v}, respectively). Therefore, $\mathcal{G}_x$ is generated by G and the d-th roots of unity, where $d=\gcd(m,r-s)$. Therefore, condition (1) is equivalent to the assertion that $u-v$ is a multiple of d, which is condition (2). This proves the theorem. □

COROLLARY 7.6. *Let $q=p^r$ be an odd prime power, where p is a prime number and where $r>1$ if $p=3$. Assume that $q\geq 11$ and $q\neq 13$. Let Θ be the unique invariant 3-tensor for $\mathrm{SL}_2(\mathbb{F}_q)$ on V_ν^ε. If q is not congruent to 1 modulo 6 then every invariant of $\mathrm{SL}_2(\mathbb{F}_q)\cdot\mathrm{Aut}(\mathbb{F}_q)$ on V_ν^ε arises from a covariant of Θ. If q is congruent to 1 modulo 6 then every invariant of degree divisible by 3 on V_ν^ε arises from Θ.*

PROOF. This follows at once from Theorems 7.3 and 7.4 and and from the fact (see [Adler 1994]) that the group $\rho_\nu^\varepsilon(\mathrm{SL}_2(\mathbb{F}_q)\cdot\mathrm{Aut}(\mathbb{F}_q))$ is the precise automorphism group of Θ modulo scalars. □

THEOREM 7.7. *Assume that $\eta=1$ and let $n=(q-\varepsilon)/2$. Then there is a cubic contravariant of n-ary cubics which does not vanish on Θ. In particular, there* ***exists*** *a nonzero cubic contravariant of n-ary cubics.*

PROOF. This follows at once from Theorem 7.5. Alternatively, by Theorem 7.4, the orbit of Θ is closed. In Theorem 7.1, let G be $\mathrm{SL}_n(\mathbb{C})$, V be the space of n-ary cubics, W be the dual space of V, x be Θ and let y be the differential operator D_Θ. By Theorem 7.1 there is a polynomial mapping λ of V into W which maps x onto y. Write λ as the sum $\lambda_0+\lambda_1+\cdots$ of its homogeneous components. Then each component is $\mathrm{SL}_n(\mathbb{C})$ invariant and is therefore a cubic contravariant of Θ. Since $\lambda(\Theta)=D_\Theta$, one of the terms $\lambda_i(\Theta)$ must be nonzero. Since any representation of $\mathrm{SL}_2(\mathbb{F}_q)$ of degree n has a unique cubic invariant (up to a scalar), we conclude that $\lambda_i(\Theta)$ must be a scalar multiple of D_Θ. Multiplying λ_i by the reciprocal of that scalar we obtain a cubic contravariant of n-ary cubics whose value on Θ is D_Θ. □

THEOREM 7.8. *Suppose q is a an odd prime which is ≥ 11 and $\neq 13$. Then the modular curve $X(q)$ may be constructed geometrically from the 3-tensor Θ in the set theoretic sense. More precisely, if $\varepsilon=1$ then the A-curve may be constructed from the restriction $\Theta|V^+$ of Θ to V^+, while if $\varepsilon=-1$, the z-curve may be constructed from the restriction $\Theta|V^-$ of Θ to V^-.*

PROOF. Note that the invariants of $\mathrm{SL}_2(\mathbb{F}_q)$ separate orbits of $\mathrm{SL}_2(\mathbb{F}_q)$. It follows that the modular curve is the set theoretic intersection of all of the invariant hypersurfaces containing it. To prove the theorem, it therefore suffices to show that every $\mathrm{SL}_2(\mathbb{F}_q)$ invariant hypersurface Z arises set theoretically as a covariant of Θ. For set theoretic purposes, we may replace any invariant by its cube. Therefore, we can assume that the degree of the form F defining Z is divisible by 3. The theorem now follows from Corollary 7.6. □

8. Appendix: The Fundamental Intertwining Operator

In this section, we recall the Weil representation of a finite symplectic group and discuss a certain intertwining operator introduced in [Adler and Ramanan 1996]. We begin by recalling some of the notation of the fundamental paper [Weil 1964] and some of our own modifications of it.

8.1. Throughout this section, G will denote a locally compact abelian group, G^* its dual group and $\mathbb{T}$ the multiplicative group of all complex numbers of absolute value 1. The natural pairing between elements $g \in G$ and $g^* \in G^*$ is denoted $\langle g, g^* \rangle$ and the operation in G^* is also written additively. We will also assume that multiplication by 2 is an automorphism of G. Weil defines the group $A(G)$ to be the set $G \times G \times \mathbb{T}$ with the group law defined by

$$(g_1, g_1^*, t_1)(g_2, g_2^*, t_2) = (g_1 + g_2, g_1^* + g_2^*, \langle g_1, g_2^* \rangle t_1 t_2).$$

The group $A(G)$ is a locally compact topological group with the product topology. Its center is $\mathbb{T}$.

8.2. We note that the same construction will define a group if $\mathbb{T}$ is replaced by any subgroup $\mathbb{T}_0$ of $\mathbb{T}$ containing all of the values $\langle g, g^* \rangle$ with $g \in G$ and $g^* \in G^*$. Thus, we obtain a group which we denote $A_0(G)$ whose underlying set is $G \times G^* \times \mathbb{T}_0$. If $\mathbb{T}_0$ is not all of $\mathbb{T}$, we give $\mathbb{T}_0$ the discrete topology, so that $A_0(G)$ is likewise a locally compact topological group. Its center is $\mathbb{T}_0$. In practice, we will take $\mathbb{T}_0$ to be the smallest subgroup containing all of the values $\langle g, g^* \rangle$. In our applications, we will often find it better to work with the group $A_0(G)$ rather than $A(G)$.

8.3. Weil constructs certain automorphisms of $A(G)$ which induce the identity on the center $\mathbb{T}$ of $A(G)$. They are as follows.

8.3.1. *The automorphism $t_0(f)$ of $A(G)$.* By a *second degree character* of a locally compact abelian group H, we will mean a function f from H in to the circle group $\mathbb{T}$ such that the mapping $\beta : H \times H \to \mathbb{T}$, given by

$$\beta(g, h) = \frac{f(g+h)}{f(g)f(h)},$$

is a character of H in each variable separately. Thus, a second degree character is analogous to a quadratic polynomial without constant term. Indeed, if $p : \mathbb{R}^n \to \mathbb{R}$ is such a quadratic polynomial then the function $exp(2\pi i p)$ is a quadratic character.

If f is a second degree character of G, denote by $\rho : G \to G^*$ the associated symmetric morphism defined by

$$\langle g, h\rho \rangle = \frac{f(g+h)}{f(g)f(h)}.$$

Note that the homomorphism ρ is written on the right in Weil's notation. The automorphism $t_0(f)$ of $A(G)$ is defined by

$$t_0(f)(g,g^*,t)=(g,g\rho+g^*,f(g)t).$$

In practice, we will be concerned with the case in which f is even, that is, $f(g)=f(-g)$ for all $g\in G$. Since multiplication by 2 is assumed to be an automorphism of G, one can show that an even second degree character f is of the form

$$f(g)=\langle g/2,g\rho\rangle$$

where $g/2$ denotes the unique element of G such that $g/2+g/2=g$ and where ρ, as above, is the symmetric morphism associated to f.

8.3.2. *The automorphism* $d_0(\alpha)$. If α is a continuous automorphism of G, the automorphism $d_0(\alpha)$ of $A(G)$ is defined by

$$d_0(\alpha)(g,g^*,t)=(g\alpha,g^*{\alpha^*}^{-1},t).$$

Here α^* is the automorphism of G^* defined by composition with α, that is,

$$\langle g\alpha,g^*\rangle=\langle g,g^*\alpha^*\rangle$$

for all $g\in G$ and all $g^*\in G^*$.

8.3.3. *The automorphism* $d_0'(\alpha)$. Let $\gamma:G^*\to G$ be an isomorphism. We will be dealing with self-dual groups G, so this construction will not be empty. The automorphism $d_0'(\gamma)$ of $A(G)$ is defined by

$$d_0'(\gamma)(g,g^*,t)=(g^*\gamma,-g{\gamma^*}^{-1},\langle g,-g^*\rangle t).$$

Here $\gamma^*:G^*\to G$ is the isomorphism defined by

$$\langle g^*\gamma^*,h^*\rangle=\langle h^*\gamma,g^*\rangle$$

for all $g^*,h^*\in G^*$.The reader can easily verify that each of these automorphisms leaves the group $A_0(G)$ invariant and induces an automorphism on $A_0(G)$.

8.4. Weil denotes by $B(G)$ the group of all continuous automorphisms of $A(G)$. Each such automorphism induces an automorphism of the center $\mathbb{T}$ of $A(G)$. Such an automorphism must either be the identity on $\mathbb{T}$ or else must induce on $\mathbb{T}$ the automorphism $t\mapsto t^{-1}$. Weil denotes by $B_0(G)$ the subgroup of $B(G)$ inducing the identity automorphism on the subgroup $\mathbb{T}$. It is then easy to see that the elements of $B(G)$ and of $B_0(G)$ actually leave invariant the group $A_0(G)$ and induce automorphisms on it. Elements of $B_0(G)$ are uniquely determined by their restrictions to $B_0(G)$. Furthermore, any automorphism of $A_0(G)$ inducing the identity on $\mathbb{T}_0$ extends uniquely to an element of $B_0(G)$. So we will be free to identify $B_0(G)$ with the group of automorphisms of $A_0(G)$ inducing the identity on the center $\mathbb{T}_0$. It is also useful to consider certain endomorphisms of $A(G)$, and we will do so before we state Lemma 8.17.

8.5. The group $A(G)$ has a canonical unitary representation on the Hilbert space $L_2(G)$ of square integrable functions on G with respect to a Haar measure on G. That representation, denoted U, is defined as follows: if (g, g^*, t) is an element of $A(G)$ and if Φ is a square integrable function on G, then the function $\Phi' = U(g, g^*, t)\Phi$ is given by

$$\Phi'(x) = t\langle x, g^*\rangle\Phi(x+g)$$

for all $t \in G$. This notation U is slightly at variance with Weil's notation, according to which Φ' would be $tU(g, g^*)\Phi$. We find this modification of Weil's notation useful for our purposes. The representation U of $A(G)$ restricts to a representation of $A_0(G)$ on $L_2(G)$. We also denote that restriction by U.

8.6. Weil denotes by $\mathbf{A}(G)$ the image of $A(G)$ under the representation U and remarks that U induces a topological isomorphism of $A(G)$ onto $\mathbf{A}(G)$ where the latter is given the strong operator topology. Weil is consistent in the use of boldface fonts for operator versions of the groups and elements we have constructed. He denotes by $\mathbf{B}_0(G)$ the normalizer of $\mathbf{A}(G)$ in the group of all unitary operators on $L_2(G)$. He shows that there is a continuous homomorphism $\pi : \mathbf{B}_0(G) \to B_0(G)$, called the *canonical projection*, such that for all $S \in \mathbf{B}_0(G)$ and all $(g, g^*, t) \in A(G)$, we have

$$U(\pi(S)(g, g^*, t)) = S^{-1}U(g, g^*, t)S.$$

The kernel of π is the group of scalar multiplications by complex numbers of absolute value 1, which we may identify with the group $\mathbb{T}$.

8.7. Weil shows how to find elements of $\mathbf{B}_0(G)$ lying over elements of $B_0(G)$. This is in fact one of the important themes of [Weil 1964]. In the case of the elements $t_0(f)$, $d_0(\alpha)$ and $d_0'(\gamma)$ mentioned above, he gives the following elements of $\mathbf{B}_0(G)$ mapped to them respectively under the canonical projection π.

8.7.1. *The operator* $\boldsymbol{t}_0(f)$. Let f be a second degree character of G. Then the operator $\boldsymbol{t}_0(f)$ on $L_2(G)$ is defined by

$$(\boldsymbol{t}_0(f)\Phi)(x) = f(x)\Phi(x)$$

for all $\Phi \in L_2(G)$ and all $x \in G$.

8.7.2. *The operator* $\boldsymbol{d}_0(\alpha)$. Let α be an automorphism of G. Then the operator $\boldsymbol{d}_0(\alpha)$ is defined by

$$(\boldsymbol{d}_0(\alpha)\Phi)(x) = |\alpha|^{\frac{1}{2}}\Phi(x\alpha)$$

for all $\Phi \in L_2(G)$ and all $x \in G$, where $|\alpha|$ denotes the modulus of the automorphism α of the locally compact abelian group G. If X is a subset of G of finite positive measure, then the ratio of the measure of $X\alpha$ to the measure of X is $|\alpha|$. In case the group G is compact, we can take the set X to be all of G and we conclude that $|\alpha| = 1$ for a compact group.

8.7.3. *The operator* $\boldsymbol{d}_0'(\gamma)$. Let $\gamma : G^* \to G$ be an isomorphism. We define the operator $\boldsymbol{d}_0'(\gamma)$ on $L_2(G)$ by

$$(\boldsymbol{d}_0'(\gamma)\Phi)(x) = |\gamma|^{-\frac{1}{2}}\Phi^*(-x\gamma^{*-1})$$

for all $\Phi \in L_2(G)$ and all $x \in G$. Here Φ^* is the Fourier transform of Φ, defined by

$$\Phi^*(x^*) = \int_G \Phi(x) \cdot \langle x, x^* \rangle \cdot dx$$

for all $x^* \in G^*$, the integral being taken with respect to a Haar measure dx on G. Thus the definition of Φ^* depends on the choice of dx, which is only unique up to a positive real factor. Specifically, if dx is replaced by cdx for some positive real number c, the value of Φ^* is likewise multiplied by c. Once one has chosen a Haar measure on G, there is canonically associated to it a Haar measure dx^* on G^*, called the dual measure, characterized by the relation

$$\int_G |\Phi(x)|^2 dx = \int_{G^*} |\Phi^*(x)|^2 dx^*$$

for all $\Phi \in L_2(G)$. Having chosen the Haar measure dx, we can therefore consider the modulus $|\gamma|$ of the isomorphism $\gamma : G^* \to G$. If X is a measurable subset of G^* with finite positive measure, $|\gamma|$ is the ratio of the dx-measure of $X\gamma$ to the dx^*-measure of X. If the Haar measure dx is replaced by cdx, where c is a positive real, then the value of $|\gamma|$ is multiplied by c^2. Thus, one sees that although both Φ^* and $|\gamma|$ depend on the choice of dx, the definition of the operator $\boldsymbol{d}_0'(\gamma)$ does not.

8.8. The reader can verify that the canonical projection maps $\boldsymbol{t}_0(f)$, $\boldsymbol{d}_0(\alpha)$ and $\boldsymbol{d}_0'(\gamma)$ respectively to $t_0(f)$, $d_0(\alpha)$ and $d_0'(\gamma)$.

8.9. Weil also showed that in general there is no homomorphism from $B_0(G)$ to $\mathbf{B}_0(G)$ whose composition with the canonical projection is the identity on $B_0(G)$. However for certain subgroups[1] of $B_0(G)$ which he denotes $B_0(G, \Gamma)$, where Γ is a closed subgroup of G, he was able to define canonical homomorphisms from $B_0(G, \Gamma)$ to $\mathbf{B}_0(G)$ whose composition with the canonical projection is the identity on $B_0(G, \Gamma)$. In the special case where G is the adèle group of a vector space of finite dimension over an $\mathbf{A}$-field (that is, a number field or an algebraic function field in one variable over a finite field), the representation so obtained is commonly known as the *Weil representation*. In his general setting, Weil denoted his homomorphism from $B_0(G, \Gamma)$ by r_Γ. If an element of $B_0(G)$ is expressed as a product of elements of the form $t_0(f)$, $d_0(\alpha)$ and $d_0'(\gamma)$, one can take the product of the operators $\boldsymbol{t}_0(f)$, $\boldsymbol{d}_0(\alpha)$ and $\boldsymbol{d}_0'(\gamma)$ associated to these elements to obtain an element of $\mathbf{B}_0(G)$. This element depends, however, on the manner

[1]The subgroup $B_0(G, \Gamma)$ of $B_0(G)$ consists of all elements of $B_0(G)$ which leave invariant the subgroup $\Gamma \times \Gamma_* \times \mathbb{T}$ of $A(G)$, where Γ_* denotes the annihilator of Γ in G^*.

in which one writes the given element of $B_0(G)$ as a product of elements of the form $t_0(f)$, $d_0(\alpha)$ and $d_0'(\gamma)$.

8.10. Following Weil, we denote by $\mathrm{Sp}(G)$ the symplectic group of G, which by definition is the group of all continuous automorphisms of $G \times G^*$ preserving the alternating bicharacter of $G \times G^*$ given by

$$((g_1, g_1^*), (g_2, g_2^*)) \mapsto \frac{\langle g_1, g_2^* \rangle}{\langle g_2, g_1^* \rangle}.$$

Following [Adler 1989], we denote by $\mathrm{Sp}'(G)$ the centralizer of $d_0(-1_G)$ in $B_0(G)$. Since every element of $B_0(G)$ leaves $\mathbb{T}$ invariant, every such element induces an automorphism of $A(G)/\mathbb{T}$. The latter group is isomorphic to $G \times G^*$ and the induced automorphism is in fact symplectic. Therefore we have a natural homomorphism from $B_0(G)$ to $\mathrm{Sp}(G)$ and it is not difficult to show using [Weil 1964, § 5] that $\mathrm{Sp}'(G)$ is mapped isomorphically onto $\mathrm{Sp}(G)$.

8.11. In [Adler 1989], the group $\mathbf{B}_1(G)$ is defined to be the subgroup of $\mathbf{B}_0(G)$ consisting of all operators in $\mathbf{B}_0(G)$ that commute with $\boldsymbol{d}_0(-1_G)$. In Lemma 25.2 of that paper, it is shown that the canonical projection maps $\mathbf{B}_1(G)$ surjectively onto $\mathrm{Sp}'(G)$ provided the following hypothesis holds:

(E) The group $\mathrm{Sp}(G)$ is generated by the elements $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$ of $\mathrm{Sp}(G)$ with $\gamma : G^* \to G$ an isomorphism.

Denote by V^+ and V^- respectively the 1 and -1 eigenspaces of $\boldsymbol{d}_0(-1_G)$ in $L_2(G)$. It is the same to say that V^+, V^- are respectively the spaces of *even* and *odd* functions in $L_2(G)$. Since the elements of $\mathbf{B}_1(G)$ commute with $\boldsymbol{d}_0(-1_G)$, they leave V^+ and V^- invariant. If S is an element of $\mathbf{B}_1(G)$, we will denote by S^+ and S^- respectively the operators induced by S on V^+ and V^-.

8.12. For the rest of this section, we will assume that G is a finite abelian group of odd order $2N+1$. In this case, $L_2(G)$ is finite-dimensional, V^+ has dimension $N+1$ and V^- has dimension N. According to [Adler 1989, Lemma 26.1], the mapping

$$S \mapsto \chi(S) = \frac{\det(S^+)}{\det(S^-)}$$

is a character of $\mathbf{B}_1(G)$ such that $\chi(t) = t$ for all $t \in \mathbb{T}$. Denote by ϕ the homomorphism from $\mathbf{B}_1(G)$ to itself given by

$$\phi(S) = \chi(S)^{-1} S.$$

The image of ϕ is denoted by $\mathrm{Sp}''(G)$. If G satisfies hypothesis (E) then [Adler 1989, Lemma 26.2] says that the canonical projection π maps $\mathrm{Sp}''(G)$ isomorphically onto $\mathrm{Sp}(G)$. The inverse of this isomorphism is denoted r'. The representation r' is also called the Weil representation.

8.13. According to [Adler 1989, Theorem 27.1], for any second degree character f of G such that $f(-x) = f(x)$ for all $x \in G$, we have

$$r'(t_0(f)) = \boldsymbol{t}_0(f).$$

So the Weil representation r' is given by Weil's explicit lifting in this case. This is not so, however, for the elements of $\mathrm{Sp}(G)$ of the form $d_0(\alpha)$ and $d_0'(\gamma)$.

8.14. For the rest of this section, we will further specialize G by assuming that G is actually a vector space of finite dimension n over the field $\mathbb{F}_p$ with p elements. Then hypothesis (E) holds in this case. Since G is compact, the factor $|\alpha|^{\frac{1}{2}}$ in $\boldsymbol{d}_0(\alpha)$ is always equal to 1. And with respect to the self-dual Haar measure on G, the factor $|\gamma|^{-\frac{1}{2}}$ in $\boldsymbol{d}_0'(\gamma)$ is always equal to 1. So we will disregard such factors in what follows. We will also use only the unique self-dual Haar measure on G. According to [Adler 1989, Theorem 27.4], for any automorphism α of G, we have

$$r'(d_0(\alpha)) = \left(\frac{\det(\alpha)}{p}\right)\boldsymbol{d}_0(\alpha),$$

where the first factor on the right side is the quadratic residue symbol of $\det(\alpha)$ in $\mathbb{F}_p$. As for the value of r' on elements of the form $d_0'(\gamma)$, let $\gamma : G^* \to G$ be an isomorphism, let ρ be a symmetric isomorphism of G onto G^* and let α be the automorphism of G defined by $\gamma = \rho^{-1}\alpha$. Then [Adler 1989, Theorem 27.5], we have

$$\chi(\boldsymbol{d}_0(\gamma)) = \gamma(f)\left(\frac{\det(\alpha)}{p}\right),$$

where f is the second degree character of G given by

$$f(x) = \langle x/2, x\rho\rangle$$

and

$$\gamma(f) = \int_G f\,dx$$

is the integral of f with respect to the unique self-dual Haar measure on G. Since hypothesis (E) holds, the elements of $\mathrm{Sp}(G)$ of the form $t_0(f)$, $d_0(\alpha)$ and $d_0'(\gamma)$ generate $\mathrm{Sp}(G)$. Therefore, the results just quoted amount to a complete determination of the Weil representation r'.

8.15. Let ν be an integer. Denote by σ_ν the mapping from $A(G)$ to itself given by

$$\sigma_\nu(g, g^*, t) = (\nu g, g^*, t^\nu).$$

Then one can verify directly that σ_ν is a continuous endomorphism of $A(G)$. Furthermore, it clearly leaves invariant the group $A_0(G)$. We are concerned with cases in which σ_ν actually induces an automorphism of $A_0(G)$; this happens, for example, if multiplication by ν is an automorphism of G and if $\mathbb{T}_0$ doesn't contain any ν-th roots of unity other than 1. When σ_ν induces an automorphism of $A_0(G)$, we will also denote that automorphism by σ_ν, or more simply by σ in case we don't need to indicate ν. It is then clear that conjugation by σ_ν induces an automorphism s_ν of $B_0(G)$. We will also write s instead of s_ν when we do not need to refer directly to the integer ν. The automorphism σ_ν of $A_0(G)$ depends only on the congruence class of ν modulo p and we will freely refer to ν as a congruence class modulo p instead of as an integer.

8.16. Let ν be a nonzero element of $\mathbb{F}_p$. Then multiplication by ν induces an automorphism of G. Accordingly, the automorphism s_ν of $B_0(G)$ is well defined. Furthermore, since s_ν itself commutes with $d_0(-1_G)$, s_ν actually induces an automorphism of $\mathrm{Sp}(G)$. That automorphism will also be denoted s_ν. The composition of s_ν with the Weil representation r' will be denoted r'_ν. Of course, the representation r' is the same as r'_1.

Lemma 8.17. *Let f be an even second degree character of G. Let α be an automorphism of G and let $\gamma : G^* \to G$ be an isomorphism. Then*

$$\begin{aligned} r'_\nu(t_0(f)) &= r'(t_0(f^\nu)), \\ r'_\nu(d_0(\alpha)) &= r'(d_0(\alpha)), \\ r'_\nu(d'_0(\gamma)) &= r'(d'_0(\gamma/\nu)). \end{aligned}$$

Proof. Let $\rho : G \to G^*$ be the symmetric isomorphism associated to f. Then

$$f(x) = \langle x/2, x\rho\rangle$$

for all $x \in G$. Let (g, g^*, t) be an arbitrary element of $A_0(G)$. Then

$$\sigma_\nu(g, g^*, t) = (\nu g, g^*, t^\nu).$$

Therefore

$$\begin{aligned} \sigma_\nu^{-1} t_0(f)\sigma_\nu(g, g^*, t) &= \sigma_\nu t_0(f)(\nu g, g^*, t^\nu) \\ &= \sigma_\nu^{-1}(\nu g, \nu g\rho + g^*, f(\nu g)t^\nu) \\ &= (g, g\nu\rho + g^*, f(g)^\nu t) = t_0(f^\nu)(g, g^*, t), \end{aligned}$$

since f^ν is the even second degree character associated to $\nu\rho$. Therefore,

$$r'_\nu(t_0(f)) = r'(s_\nu(t_0(f))) = r'(t_0(f^\nu)).$$

Since $d_0(\alpha)$ commutes with σ_ν, we similarly have

$$r'_\nu(d_0(\alpha)) = r'(s_\nu(d_0(\alpha))) = r'(d_0(\alpha)).$$

Finally,

$$\begin{aligned} \sigma_\nu^{-1} d'_0(\gamma)\sigma_\nu(g, g^*, t) &= \sigma_\nu^{-1} d'_0(\gamma)(\nu g, g^*, t^\nu) \\ &= \sigma_\nu^{-1}(g^*\gamma, -\nu g\gamma^{*-1}, \langle g, -g^*\rangle^\nu t^\nu) \\ &= (g^*\gamma/\nu, -\nu g\gamma^{*-1}, \langle g, -g^*\rangle t) = d'_0(\gamma/\nu), \end{aligned}$$

so $r'_\nu(d_0(\gamma)) = r'(d_0(\gamma/\nu))$. $\square$

8.18. The representations r' and r'_ν of $\mathrm{Sp}(G)$ on $L_2(G)$ induce representations, also denoted respectively by r' and r'_ν, on the tensor powers of $L_2(G)$. Since we can identify $L_2(G)\otimes L_2(G)$ with $L_2(G\times G)$ canonically, in particular we obtain representations r', r'_ν of $\mathrm{Sp}(G)$ on $L_2(G\times G)$. Similarly, we will freely regard operators such as $\boldsymbol{t}_0(f)$, $\boldsymbol{d}_0(\alpha)$ and $\boldsymbol{d}'_0(\gamma)$ as operators on $L_2(G\times G)$. The identities of the preceding lemma therefore hold without modification when both sides are regarded as operators on $L_2(G\times G)$. It is useful to observe that when the number of tensor factors is a positive integer N, the factors such as $\bigl(\frac{\det(\alpha)}{p}\bigr)$ and $\gamma(f)$ are replaced by their N-th powers. Since each of these factors equals ±1, it follows that when the number of tensor factors is even, the factors become equal to 1. We will in fact be concerned with the case of two tensor factors, so we will not have to worry about these factors further. However, we also have occasion to consider tensor products of representations r'_ν for different ν. We will then use multi-indices for the subscript of r'. Explicitly, we will denote by $r'_{\mu*\nu}$ the tensor product of r'_μ and r'_ν, where μ and ν may be either single integers or multi-indices and where $*$ denotes concatenation of lists of integers.

8.19. We now introduce an operator that has proved to be of fundamental importance in our work. It is the operator $\mathcal{T}$ on $L_2(G\times G)$ given by

$$(\mathcal{T}\Phi)(x,y)=\Phi\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)$$

for all $\Phi\in L_2(G\times G)$ and all $x,y\in G$. We will refer to the operator $\mathcal{T}$ as the *fundamental intertwining operator*. We then have the following result, stated and proved in special cases in [Adler and Ramanan 1996] but undoubtedly well known, which justifies this terminology.

THEOREM 8.20. *The operator $\mathcal{T}$ is an isomorphism between the representations r' and r'_2 on $L_2(G\times G)$.*

PROOF. We will simply verify this for the elements of $\mathrm{Sp}(G)$ of the form $t_0(f)$, $d_0(\alpha)$ and $d'_0(\gamma)$. Let $\Phi\in L_2(G\times G)$ and $x,y\in G$. Then

$$\begin{aligned}
(\mathcal{T}r'_2(t_0(f))(\Phi))(x,y)&=(r'_2(t_0(f))(\Phi))\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)\\
&=(r'(t_0(f^2))(\Phi))\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)\\
&=f^2\Bigl(\frac{x+y}{2}\Bigr)f^2\Bigl(\frac{x-y}{2}\Bigr)\Phi\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)\\
&=\Bigl\langle\frac{x+y}{4},\frac{x+y}{2}2\rho\Bigr\rangle\Bigl\langle\frac{x-y}{4},\frac{x-y}{2}2\rho\Bigr\rangle\Phi\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)\\
&=\langle x/2,x\rho\rangle\langle y/2,y\rho\rangle\Phi\Bigl(\frac{x+y}{2},\frac{x-y}{2}\Bigr)\\
&=(r'(t_0(f))(\mathcal{T}\Phi))(x,y),
\end{aligned}$$

which proves the theorem in the case of $t_0(f)$. For $d_0(\alpha)$ we simply have

$$\begin{aligned}(\mathcal{T}r_2'(d_0(\alpha))(\Phi))(x,y) &= (r_2'(d_0(\alpha))(\Phi))\Big(\frac{x+y}{2},\frac{x-y}{2}\Big)\\ &= (r'(d_0(\alpha))(\Phi))\Big(\frac{x+y}{2},\frac{x-y}{2}\Big)\\ &= \Phi\Big(\frac{x+y}{2}\alpha,\frac{x-y}{2}\alpha\Big)\\ &= (\mathcal{T}(\Phi))(x\alpha,y\alpha) = (r'(d_0(\alpha))\mathcal{T}(\Phi))(x,y),\end{aligned}$$

which proves the theorem in the case of $d_0(\alpha)$. Finally, if $\gamma : G^* \to G$ is an isomorphism and $\rho : G \to G^*$ is a symmetric isomorphism, we let $\alpha = \rho\gamma$. We then have

$$\begin{aligned}&(\mathcal{T}r_2'(d_0'(\gamma))(\Phi))(x,y)\\ &\quad= (r_2'(d_0'(\gamma))(\Phi))\Big(\frac{x+y}{2},\frac{x-y}{2}\Big)\\ &\quad= (r'(d_0'(\gamma/2))(\Phi))\Big(\frac{x+y}{2},\frac{x-y}{2}\Big)\\ &\quad= \int_{G\times G}\Phi(u,v)\Big\langle u,-\frac{x+y}{2}(\gamma/2)^{*-1}\Big\rangle\Big\langle v,-\frac{x-y}{2}(\gamma/2)^{*-1}\Big\rangle\,dx\,dy\\ &\quad= \int_{G\times G}\Phi\Big(\frac{a+b}{2},\frac{a-b}{2}\Big)\Big\langle\frac{a+b}{2},-(x+y)\gamma^{*-1}\Big\rangle\Big\langle\frac{a-b}{2},-(x-y)\gamma^{*-1}\Big\rangle\,dx\,dy\\ &\quad= \int_{G\times G}\Phi\Big(\frac{a+b}{2},\frac{a-b}{2}\Big)\langle a,-x\gamma^{*-1}\rangle\langle b,-y\gamma^{*-1}\rangle\,da\,db\\ &\quad= \int_{G\times G}(\mathcal{T}\Phi)(a,b)\langle a,-x\gamma^{*-1}\rangle\langle b,-y\gamma^{*-1}\rangle\,da\,db\\ &\quad= (r'(d_0'(\gamma))\mathcal{T}(\Phi))(x,y). \qquad\square\end{aligned}$$

8.21. The subspaces V^+ and V^- are invariant under r_ν' for all integers ν. The representations one obtains on these spaces for each ν will be denoted ρ_ν^+ and ρ_ν^- respectively. Although the spaces V^+ and V^- themselves do not depend on ν, we will denote them V_ν^+ and V_ν^- respectively whenever we wish to emphasize that one is acting on them via ρ_ν^+ and ρ_ν^-. We also note that, for the purposes of studying the relevant bicycles, all of the representations r_ν' of $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ (resp. $\mathrm{SL}_2(\mathbb{F}_q)$) are equivalent under the group of automorphisms of $\mathrm{Sp}_{2r}(\mathbb{F}_p)$ (resp. $\mathrm{SL}_2(\mathbb{F}_q)$) and the representation $r_{-\nu}'$ is the dual of the representation r_ν'. The same remarks apply, *mutatis mutandis*, to the representations $\rho_\nu^\pm$. In particular, the rings of invariants of all of these representations form bicycles.

8.22. Parts of the following result, and the relevant principles for proving it, may be found in [Adler and Ramanan 1996, pp. 54, 55, 74].

LEMMA 8.23. *We have*

$$\mathcal{T}\big(\mathrm{Sym}^2(V_\nu^+)\big)=\mathrm{Sym}^2(V_{2\nu}^+),\qquad \mathcal{T}\big(\textstyle\bigwedge^2(V_\nu^-)\big)=\textstyle\bigwedge^2(V_{2\nu}^-),$$
$$\mathcal{T}\big(\mathrm{Sym}^2(V_\nu^-)\big)=\textstyle\bigwedge^2(V_{2\nu}^+),\qquad \mathcal{T}\big(\textstyle\bigwedge^2(V_\nu^+)\big)=\mathrm{Sym}^2(V_{2\nu}^-).$$

PROOF. Denote by α, β two numbers each of which is equal to ±1. Denote by $W(\alpha,\beta)$ the space of all complex valued functions $f(x,y)$ on $G\times G$ such that

$$f(y,x)=\alpha f(x,y)$$

and

$$f(-x,y)=\beta f(x,y).$$

We note that these two conditions imply

$$f(x,-y)=\beta f(x,y).$$

We then have

$$W(\ \ 1,1)=\mathrm{Sym}^2(V_{2\nu}^+),\qquad W(\ \ 1,-1)=\mathrm{Sym}^2(V_{2\nu}^-),$$
$$W(-1,1)=\textstyle\bigwedge^2(V_{2\nu}^+),\qquad W(-1,-1)=\textstyle\bigwedge^2(V_{2\nu}^-).$$

If $f\in W(\alpha,\beta)$, then

$$(\mathcal{T}f)(y,x)=f\Big(\frac{y+x}{2},\frac{y-x}{2}\Big)=\beta f\Big(\frac{y+x}{2},\frac{x-y}{2}\Big)=\beta(\mathcal{T}f)(x,y)$$

and

$$(\mathcal{T}f)(-x,y)=f\Big(\frac{-x+y}{2},\frac{-x-y}{2}\Big)=f\Big(\frac{x-y}{2},\frac{x+y}{2}\Big)=\alpha f\Big(\frac{x+y}{2},\frac{x-y}{2}\Big).$$

This shows that $\mathcal{T}$ maps $W(\alpha,\beta)$ into $W(\beta,\alpha)$. Since $L_2(G\times G)$ is finite-dimensional and is the direct sum of the spaces $W(\alpha,\beta)$, we are done. □

8.24. We can generalize the fundamental intertwining operator in the following way. Let a,b be any elements of $\mathbb{F}_p$ such that $a^2+b^2\neq 0$. Then we define the operator $\mathcal{T}_{a,b}$ on $L^2(G\otimes G)$ by the rule

$$(\mathcal{T}_{a,b}\Phi)(x,y)=\Phi(ax+by,-bx+ay).$$

A computation similar to the one in Theorem 8.20 shows that $\mathcal{T}_{a,b}$ is an intertwining operator between the representations r'_ν and $r'_{\nu(a^2+b^2)}$ on $L^2(G\times G)$, that is,

$$\mathcal{T}_{a,b}\circ r'_\nu=r'_{\nu(a^2+b^2)}\circ\mathcal{T}_{a,b}.$$

The fundamental intertwining operator is then $\mathcal{T}_{\frac12,\frac12}$. We do need the more general interwining operator $\mathcal{T}_{a,b}$ in Section 4, for example. It should be noted that the preceding lemma does not hold in general with $\mathcal{T}$ replaced by $\mathcal{T}_{a,b}$, but it does hold if $a=b$.

8.25. We can identify the group $\mathrm{Sp}(G)$ with the finite symplectic group $\mathrm{Sp}_{2s}(\mathbb{F}_p)$, where the order of G is p^{2s}. If $s = nr$, where n, r are positive integers, the group $\mathrm{Sp}_{2n}(\mathbb{F}_q)$, where $q = p^r$, is naturally a subgroup of $\mathrm{Sp}_{2s}(\mathbb{F}_p)$. The Weil representations of $\mathrm{Sp}(G)$ therefore give rise to representations of these two groups which we also refer to as Weil representations. We will also retain the notations r' and r'_ν.

8.26. By drawing on the methods and concepts of [Weil 1964, § 49], the results of this Appendix can be extended without difficulty to treat the Weil representation of the symplectic group $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ directly. Instead of the group $A_0(G)$, one introduces the group $A^\#(G)$ whose underlying point set is $G \times G^* \times \mathbb{F}_q$ and whose operation is given by

$$(g_1, g_1^*, u_1)(g_2, g_2^*, u_2) = (g_1 + g_2,\ g_1^* + g_2^*,\ [g_1, g_2^*] + u_1 + u_2).$$

In order to explain the pairing $[\,\cdot\,,\cdot\,]$ that appears on the right, denote by tr the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ and by τ the character of the additive group of $\mathbb{F}_q$ given by

$$\tau(x) = \zeta_p^{\mathrm{tr}(x)}.$$

There is a natural structure on G^* of vector space over $\mathbb{F}_q$ induced by that of G. Denote by G' the dual space of the $\mathbb{F}_q$ vector space G. There is a canonical isomorphism of G' onto G^* which associates to an element λ of G' the composition $\tau \circ \lambda$ of λ and τ. By means of this isomorphism, we canonically identify G^* with G'. The pairing $[\,\cdot\,,\cdot\,]$ is then the natural pairing from $G \times G'$ to $\mathbb{F}_q$.

8.27. We identify $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ with the centralizer in $\mathrm{Sp}(G)$ of all elements of the form $d_0(\alpha)$ where α is scalar multiplication by an element of $\mathbb{F}_q$. One can then verify that $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ acts as a group of automorphisms of $A^\#(G)$ in a natural way. Explicitly, suppose an element β of $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ acts on $A_0(G)$ by the rule

$$(w, t) \mapsto (w\beta, f(w)t),$$

where $w \in G \times G^*$ and where f is a second degree character of G such that $f(-x) = f(x)$ for all $x \in G$. Then as in [Weil 1964, § 49] we can write f uniquely in the form

$$f(x) = \tau(F(x)),$$

where $F : G \times G^* \to \mathbb{F}_q$ is a quadratic form on the $\mathbb{F}_q$ vector space $G \times G^*$. Then β acts on $A^\#(G)$ by

$$\beta(w, u) = (w\beta, u + F(w)).$$

8.28. If ν is a nonzero element of $\mathbb{F}_q$, we can define the automorphism σ_ν of $A^\#(G)$ by the rule

$$\sigma_\nu(g, g^*, u) = (\nu g, g^*, \nu u).$$

Conjugation by σ_ν leaves $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ invariant and induces an automorphism on it which we denote s_ν. We denote by r'_ν the composition of the Weil representation r' with s_ν. Thus, we can obtain more Weil representations of $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ in this way than we could using only integers ν prime to p. The importance of considering these more general Weil representations is that in case ν happens to be a square in $\mathbb{F}_q$, the Weil representation is equivalent to the original Weil representation. If $q = p^r$ with r even, then every element of $\mathbb{F}_p$ will be a square in $\mathbb{F}_q$ and we will get nothing new. But by taking ν to be an element of $\mathbb{F}_q$ which is not a square in $\mathbb{F}_q$, we do get something new.

8.29. In connection with the bicycles we are considering, note that even if ν is not a square in $\mathbb{F}_q$, the Weil representation r'_ν can be obtained from r' by composition with an automorphism of $\mathrm{Sp}_{2n}(\mathbb{F}_q)$.

8.30. With these preliminaries, the fundamental intertwining operator still behaves as described in Lemma 8.23 and the intertwining operators $\mathcal{T}_{a,b}$ can be defined more generally whenever a, b are elements of $\mathbb{F}_q$ such that $a^2 + b^2 \neq 0$.

8.31. In closing, we show that if -1 is a square in $\mathbb{F}_q$ then the representation of $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ on V_ν^+ is orthogonal and on V_ν^- is symplectic. Since -1 is a square, let a be a square root of -1 in $\mathbb{F}_q$. Then the mapping τ_a from $L_2(\mathbb{F}_q)$ to itself given by

$$\tau_a \Phi(x) = \Phi(ax)$$

normalizes $r'(\mathrm{Sp}_{2n}(\mathbb{F}_q))$. Indeed, an easy direct computation shows that τ_a intertwines r'_ν and $r'_{-\nu}$. On the other hand, we have the canonical $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ invariant pairing between r'_ν and $r'_{-\nu}$ given by

$$\langle \Phi_1, \Phi_2 \rangle = \sum \Phi_1(x)\Phi_2(x),$$

where the summation runs over all $x \in \mathbb{F}_q^n$. We therefore obtain the bilinear pairing $\mathcal{Q}$ on $L_2(\mathbb{F}_q^n)$ given by

$$\mathcal{Q}(\Phi_1, \Phi_2) = \sum \Phi_1(x)\Phi_2(ax).$$

If Φ_1, Φ_2 are even functions on $\mathbb{F}_q^n$, we have

$$\mathcal{Q}(\Phi_2, \Phi_1) = \mathcal{Q}(\Phi_1, \Phi_2),$$

hence the restriction $\mathcal{Q}^+$ of $\mathcal{Q}$ to V_ν^+ is symmetric. One sees that it is also nonzero by taking $\Phi_1 = \Phi_2$ to be the function which is 1 at 0 and 0 everywhere else. This shows that V_ν^+ is orthogonal and gives the invariant quadratic form explicitly as

$$\Phi \mapsto \sum \Phi(x)\Phi(ax).$$

We will also denote this quadratic form by $\mathcal{Q}^+$. On the other hand, if Φ_1, Φ_2 are both odd functions on $\mathbb{F}_q^n$, we have

$$\mathcal{Q}(\Phi_2, \Phi_1) = -\mathcal{Q}(\Phi_1, \Phi_2),$$

which shows that the restriction $\mathcal{Q}^-$ of $\mathcal{Q}$ to V_ν^- is alternating. To see that it is nonzero, let y be a nonzero element of $\mathbb{F}_q^n$ and let Φ_1 be 1 at y, -1 at $-y$ and 0 everywhere else and let $\Phi_2(x) = \Phi_1(ax)$ for all x. Then we have

$$\mathcal{Q}^-(\Phi_1, \Phi_2) = \sum \Phi_1(x)\Phi_2(ax) = -\sum \Phi_1(x)^2 = -2,$$

which proves that $\mathcal{Q}^-$ is also nonzero. Thus V_ν^- is symplectic and its invariant alternating form $\mathcal{Q}^-$ is given explicitly.

Acknowledgements

I am grateful to Gerry Schwarz and to David Vogan for their crucial help with the results of Section 7 and to Ofer Gabber for pointing out a simple oversight in the formulation of the Bicycle Conjecture. I am also thankful to IHES for lodging during the second half of 1994 and for support during the fall of 1994, as well as for allowing me to conduct an informal seminar that provided the crucial stimulation I needed to make final revisions in the manuscript. I am especially grateful to Mischa Gromov, Marcel Berger and Jean-Pierre Bourguignon for their sympathetic help in making the facilities of IHES available to me.

References

[Adler 1981] A. Adler, "On the ring of invariants of $\mathrm{PSL}_2(\mathbf{F}_{11})$ acting on $\mathbf{C}^5$", preprint, Tata Institute, Bombay, 1981.

[Adler 1989] A. Adler, "On the Weil representation", preprint, 1989. Reprinted as [Adler and Ramanan 1996, Appendix 1].

[Adler 1992a] A. Adler, "Cubic invariants for $\mathrm{SL}_2(\mathbf{F}_q)$", *J. Algebra* **145**:1 (1992), 178–186.

[Adler 1992b] A. Adler, "Invariants of $\mathrm{PSL}_2(\mathbf{F}_{11})$ acting on $\mathbf{C}^5$", *Comm. Algebra* **20**:10 (1992), 2837–2862.

[Adler 1994] A. Adler, "On the automorphism groups of certain hypersurfaces, II", *Comm. Algebra* **22**:7 (1994), 2319–2366.

[Adler 1997] A. Adler, "The Mathieu group M_{11} and the modular curve $X(11)$", *Proc. London Math. Soc.* (3) **74**:1 (1997), 1–28.

[Adler and Ramanan 1996] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Math. **1644**, Springer, Berlin, 1996.

[Baker 1935] H. F. Baker, "Note introductory to the study of Klein's group of order 168", *Proc. Camb. Phil. Soc.* **31** (1935), 168–181.

[Burckhardt 1893] H. Burckhardt, "Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunktionen III", *Mathematische Annalen* **41** (1893), 313.

[Coble 1917] A. Coble, "Point sets and allied Cremona groups, III", *Trans. Amer. Math. Soc.* **18** (1917), 331–372.

[Dieudonné and Carrell 1971] J. A. Dieudonné and J. B. Carrell, *Invariant theory, old and new*, Academic Press, New York, 1971. Alternatively see article of the same name in *Advances in Math.* **4** (1970), 1–80.

[Edge 1947] W. L. Edge, "The Klein group in three dimensions", *Acta Math.* **79** (1947), 153–223.

[Grace and Young 1903] J. H. Grace and A. Young, *The algebra of invariants*, University Press, Cambridge, 1903. Reprinted by G. E. Stechert, New York, 1941 and by Chelsea, Bronx, NY, 1965.

[Klein 1879a] F. Klein, "Ueber die Transformationen siebenter Ordnung der elliptischen Funktionen", *Math. Annalen* **14** (1879), 428–471. Reprinted as [Klein 1923, LXXXIV, pp. 90–136]. Translated in this collection.

[Klein 1879b] F. Klein, "Ueber die Transformation elfter Ordnung der elliptischen Modulfunktionen", *Math. Annalen* **15** (1879), 533–555. Reprinted as [Klein 1923, LXXXVI, pp. 140–168].

[Klein 1923] F. Klein, *Gesammelte Mathematische Abhandlungen, 3: Elliptische Funktionen* etc., edited by R. Fricke et al., Springer, Berlin, 1923. Reprinted by Springer, 1973.

[Klein and Fricke 1890–92] F. Klein, *Vorlesungen über die Theorie der elliptischen Modulfunctionen,* ausgearbeitet und vervollständigt von Robert Fricke (2 vol.), Teubner, Leipzig, 1890–92. Reprinted by Johnson Reprint, New York, 1966.

[Levasseur and Stafford 1995] T. Levasseur and J. T. Stafford, "Invariant differential operators and an homomorphism of Harish-Chandra", *J. Amer. Math. Soc.* **8**:2 (1995), 365–372.

[Luna 1975] D. Luna, "Adhérences d'orbite et invariants", *Invent. Math.* **29**:3 (1975), 231–238.

[Wallach 1993] N. R. Wallach, "Invariant differential operators on a reductive Lie algebra and Weyl group representations", *J. Amer. Math. Soc.* **6**:4 (1993), 779–816.

[Weil 1964] A. Weil, "Sur certains groupes d'opérateurs unitaires", *Acta Math.* **111** (1964), 143–211. Reprinted as pp. 1–69 in his *Collected Papers*, vol. III, Springer, New York, 1979.

Allan Adler
P.O.Box 1043
Bowling Green, KY 42102-1043
United States
adler@hera.wku.edu