ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 28, Number 1, Spring 1998

TWIN SEXTIC ALGEBRAS

DAVID P. ROBERTS

0. Introduction. Among all the symmetric groups, only S_6 has a nontrivial outer automorphism group, it being $\mathrm{Out}\,(S_6) = \{1, t\}$. Because of the exceptional involution t, a sextic separable algebra K over a ground field F has a "twin" K^t, well-defined up to unique isomorphism. The double twin K^{tt} is canonically isomorphic to the given algebra K. It may very well happen that K is a field but its twin K^t is not.

This paper presents a large number of facts, very useful to have at hand when one is investigating sextic algebras over a given ground field. We review the exceptional twinning operation in some detail. Also in our discussion of other topics, we continue to emphasize the helpful role played by this operation. The results presented in this paper are used in [**11**] for p-adic ground fields $F = \mathbf{Q}_p$ and in [**7**] for the rational ground field $F = \mathbf{Q}$.

Section 1 reviews the categorical approach to Galois theory; it is essential to take this approach because we must deal with algebras, not just fields. Section 2 centers upon simply giving the classical lists of possible Galois groups of sextic algebras: there are 40 intransitive groups, corresponding to nonfields, and 16 transitive groups, corresponding to fields. Here, in an effort to render the list as intelligible as possible, we organize the intransitive groups according to their "product closures."

Section 3 presents group-theoretic facts about the exceptional outer automorphism t of S_6. Then it discusses a basic formula due to Girstmair [**4**]; this formula explicitly associates to a polynomial f with $K = F[x]/f$ a new polynomial f^t which, if separable, satisfies $K^t = F[x]/f^t$. For comparison we also give a new much simpler twinning formula for an important special case.

Section 4 tabulates a wealth of explicit facts about the conjugacy classes and characters of the 56 groups in question; here the role played by t is emphasized constantly. Finally in Section 5 we give a geometric

Received by the editors on December 11, 1995.

collection of examples, intended to complement the p-adic and number-theoretic examples mentioned above. Here the ground field is $F = \mathbf{C}(t)$ but the presentation is in terms of covers of the complex projective line $\mathbf{P}^1$, ramified only in $\{0, 1, \infty\}$.

1. Categorical Galois theory. Let F be a field. Galois theory is usually presented from an "internal" point of view. Namely, one fixes a Galois extension field F' of F, often a separable closure, and studies subfields K of F' of finite degree over F. Here we review the less well-known "categorical" point of view, where one studies finite-dimensional separable algebras over F. The difference between the internal and categorical viewpoint is very slight, but in many respects crucial.

Let $\mathrm{Alg}\,(F)$ be the category of finite-dimensional separable algebras over F. Let $V_0(F)$ be the category of smooth zero-dimensional varieties over F. The contravariant functor

$$\mathrm{Spec} : \mathrm{Alg}\,(F) \longrightarrow V_0(F)$$

is an antiequivalence of categories. Here, out of deference to the classical point of view in Galois theory, we will work mostly with $\mathrm{Alg}\,(F)$ rather than $V_0(F)$. However, the geometric point of view is better for some purposes; Section 5 is written in this alternative language.

Let $\mathrm{Field}(F) \subset \mathrm{Alg}\,(F)$ be the subcategory consisting of fields. Via the spectrum functor this subcategory corresponds to $V_0^{\mathrm{conn}}(F)$, the category of connected zero-dimensional varieties over F. Of course, every object in $V_0(F)$ is a finite direct sum, i.e., disjoint union, of objects in $V_0^{\mathrm{conn}}(F)$. In this sense the passage from fields to algebras should not be considered an increase in generality. Rather it is an increase in functoriality, the most important point being that $V_0^{\mathrm{conn}}(F)$ is not closed under direct product.

Let $\overline{F}$ be a separable closure of F. An algebra K with spectrum X then determines a finite set

$$X(\overline{F}) = \mathrm{Hom}_F(K, \overline{F}).$$

By post-composition the usual absolute Galois group $\mathrm{Gal}(\overline{F}/F) = \mathrm{Aut}(\overline{F}/F)$ acts from the left on $X(\overline{F})$. The following statement is

the main theorem of Galois theory. *The functor*

$$\begin{array}{ccc} \textit{Smooth zero-dimensional } F\textit{-varieties} & \longmapsto & \textit{Finite } \mathrm{Gal}(\overline{F}/F)\textit{-sets} \\ X & \longmapsto & X(\overline{F}) \end{array}$$

is an equivalence of categories. Under this equivalence, connected varieties correspond to transitive $\mathrm{Gal}(\overline{F}/F)$-sets.

The Galois group $\mathrm{Gal}(K, \overline{F})$ is by definition the image of $\mathrm{Gal}(\overline{F}/F)$ in the symmetric group $\mathrm{Sym}\,(X(\overline{F}))$. To clarify this definition, let $\overline{F}^K$ be the compositum of the images of all F-homomorphisms from K to $\overline{F}$; then, as an abstract group, $\mathrm{Gal}(K, \overline{F}) = \mathrm{Gal}(\overline{F}^K/F) = \mathrm{Aut}(\overline{F}^K/F)$.

By pre-composition, the usual automorphism group $\mathrm{Aut}(K)$ acts from the right on $X(\overline{F}) = \mathrm{Hom}(K, \overline{F})$. So its opposite group $\mathrm{Aut}(X)$ acts from the left on $X(\overline{F})$. The fundamental picture is thus

$$\mathrm{Gal}(K, \overline{F}) \subseteq \mathrm{Sym}\,(X(\overline{F})) \supseteq \mathrm{Aut}(X),$$

the Galois and automorphism groups obviously commuting with one another; in fact, $\mathrm{Aut}(X)$ is the centralizer of $\mathrm{Gal}(K, \overline{F})$.

Here are two comments which should help clarify the distinction between $\mathrm{Gal}(K, \overline{F})$ and $\mathrm{Aut}(X)$. First, $\mathrm{Aut}(X)$ is a group canonically associated to the algebra K while $\mathrm{Gal}(K, \overline{F})$ depends on the auxiliary choice of $\overline{F}$. Second, in some extreme examples the situation is as follows. If K is a direct sum of n copies of F, then $\mathrm{Gal}(K, \overline{F}) = \{e\}$ and $\mathrm{Aut}(X) \cong S_n$. If K is a degree $n \geq 3$ field extension of F with $\mathrm{Gal}(K, \overline{F}) \cong S_n$, then $\mathrm{Aut}(X) = \{e\}$.

Suppose now that K is a field so that the $\mathrm{Gal}(K, \overline{F})$ action is transitive. Then one has

$$|\mathrm{Gal}(K, \overline{F})| \geq [K : F] \geq |\mathrm{Aut}(X)|,$$

the inequalities being either both strict or both equalities. In the latter case, i.e., in the case when K/F is Galois, the field $\overline{F}^K$ is the image of each of the embeddings in $\mathrm{Hom}(K, \overline{F})$. The choice of a point $x \in X(\overline{F})$ gives an isomorphism $\sigma_x : K \to \overline{F}^K$. So this choice gives an isomorphism

$$\begin{array}{ccc} \pi_x : \mathrm{Gal}(K, \overline{F}) & \xrightarrow{\sim} & \mathrm{Aut}(X) \\ \sigma & \longmapsto & \sigma_x^{-1}\sigma^{-1}\sigma_x. \end{array}$$

Here we are implicitly using the identifications $\mathrm{Gal}(K, \overline{F}) = \mathrm{Aut}(\overline{F}^K)$ and $\mathrm{Aut}(X) = \mathrm{Aut}(K)^{\mathrm{opp}}$. Exactly in the case where $\mathrm{Gal}(K, \overline{F})$ is abelian do all these isomorphisms π_x coincide; exactly in this abelian case do $\mathrm{Gal}(K, \overline{F})$ and $\mathrm{Aut}(X)$ coincide as subgroups of $\mathrm{Sym}\,(X(\overline{F}))$.

One senses a duality between $\mathrm{Gal}(K, \overline{F})$ and $\mathrm{Aut}(X)$ because they commute with one another. Here is one situation in which this rough duality is felt very strongly. Consider simultaneously $\mathbf{Q}$ and its completion $\mathbf{Q}_p$ at a prime p. Choose compatible algebraic closures: $\overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_p$. Then $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ is naturally a subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Now let K be a $\mathbf{Q}$-algebra with completion the $\mathbf{Q}_p$-algebra K_p. Then one has reverse inclusions of subgroups of $\mathrm{Sym}\,(X(\overline{\mathbf{Q}})) = \mathrm{Sym}\,(X(\overline{\mathbf{Q}}_p))$:

$$\begin{aligned} \mathrm{Gal}(K, \overline{\mathbf{Q}}) &\supseteq \mathrm{Gal}(K_p, \overline{\mathbf{Q}}_p) \\ \mathrm{Aut}(X) &\subseteq \mathrm{Aut}(X_p). \end{aligned}$$

In other words, Galois groups decrease under completion while automorphism groups increase. This duality holds in the setting of an arbitrary base-field extension F'/F, not just for those extensions like $\mathbf{Q}_p/\mathbf{Q}$ coming from completion.

A typical situation in practice is that one is given F and K but one never chooses a separable closure $\overline{F}$. Then one still has a group, now well-defined only up to conjugation, which we denote by $\mathrm{Gal}(K)$: by definition $\mathrm{Gal}(K)$ is just any $\mathrm{Gal}(K, \overline{F})$. Standard inner invariants, such as the set of conjugacy classes $\mathrm{Gal}(K)^\natural$, and the set of irreducible characters $\widehat{\mathrm{Gal}(K)}$, are completely well-defined. In practice, much of Galois theory takes place at this level.

The point of view towards Galois theory just summarized is in some ways a throwback to the original point of view of Galois. Suppose that K is given as usual by a single separable polynomial f:

$$K = F[x]/f.$$

Then $X(\overline{F})$ is naturally identified with the set of roots of f in $\overline{F}$. The Galois group $\mathrm{Gal}(K, \overline{F})$ is then the group of "allowed" permutations of the roots, i.e., permutations that preserve all algebraic relations. To our knowledge, the categorical point of view was first aggressively pursued by Grothendieck. See [**6**] or, e.g., the short summary [**10**, pp.

39–45]. It is the required point of view when one views Galois theory as part of Grothendieck's motivic Galois theory.

2. Subgroups of S_6. Let K be a degree n separable algebra over a ground field F. The Galois group $\mathrm{Gal}(K)$ then gives a subgroup of S_n, well-defined up to conjugation. Motivated in part by this connection with Galois theory, several mathematicians in the 1800's worked on drawing up complete lists of conjugacy classes of subgroups of S_n. In the sequel the words "conjugacy classes of" will not be repeated, being implicit throughout.

The following table is based on information in [**9**, pp. 1–9]. It gives for $n \leq 10$ the number of subgroups of various types, the notion "product" being explained below.

Degree	n	0	1	2	3	4	5	6	7	8	9	10
Transitive	t_n	0	1	1	2	5	5	16	7	50	34	45
Product	p_n	1	1	2	4	10	17	42	66	166	285	554
All	a_n	1	1	2	4	11	19	56	96	296	554	1593

It is somewhat remarkable that the nineteenth century authors focused on the general case, corresponding to algebras, rather than restricting to the much easier transitive case, corresponding to fields. For a lively historical account of this activity, written by one of the principal later participants, see Miller's note cited above.

The 40 *intransitive subgroups of* S_6. The following chart lists the 40 intransitive subgroups of S_6. They are organized firstly according to the partition of 6 induced by the orbit partition of $\{1, 2, 3, 4, 5, 6\}$. Throughout we omit superfluous ones; thus 5 stands for the partition 51 and S_5 could well be rewritten S_5S_1, Cartesian products being always written as juxtaposition.

The groups are organized secondly according to their "product closures." Here suppose G acts on X with orbits X_i. Let the image of G in $\mathrm{Sym}\,(X_i)$ be G_i; so G_i is a transitive subgroup of $\mathrm{Sym}\,(X_i)$. The product closure of G is by definition $\prod G_i$. So according to the above chart, there are $42 - 16 = 26$ intransitive product-closed subgroups of

S_6. There are thus $40 - 26 = 14$ nonproduct-closed subgroups.

The first five lines can be reinterpreted as giving the transitive subgroups of S_1 through S_5. Here C stands for cyclic, D for dihedral, F for Frobenius, A for alternating, and S for symmetric. These groups exist for every n, the orders being n, $2n$, $\phi(n)n$, $n!/2$ and $n!$, respectively. Here perhaps the least familiar are the Frobenius groups; F_n is the group of permutations of $\mathbf{Z}/n$ of the form $x \mapsto mx + b$ with $m \in (\mathbf{Z}/n)^\times$ and $b \in \mathbf{Z}/n$. In our setting $n \leq 5$ there are many degeneracies, e.g., $D_4 = F_4$. Past the single further degeneracy $D_6 = F_6$ these five groups are always distinct. The one group on the above list not of the form so far discussed is $V = V_4$, the noncyclic group of order four.

Each subsequent line beginning with a partition gives the corresponding product groups; these are trivial to obtain from the previously listed transitive groups. Beneath each product group H are the remaining groups having H as product closure. The notation $A^h B$ means the following: implicitly there is a third group C with surjections $h_A : A \to C$ and $h_B : B \to C$; then

$$A^h B = \{(a, b) \in A \times B : h_A(a) = h_B(b)\}$$

is the associated fiber product.

When the symbol h is "+" the group C has two elements. Both A and B are odd permutation groups and the homomorphisms h_A and h_B are the sign characters. These groups have an equally simple alternative description:

$$A^+ B = (AB) \cap A_6.$$

When the symbol h is "Δ," then A, B and C are all isomorphic. Thus, for example, S_3 indicates a six-element subgroup of S_6 with orbit partition 3111; on the other hand $S_3^\Delta S_3$ indicates an isomorphic six-element subgroup with orbit partition 33.

The groups with product closure $D_4 C_2$ require a comment. The transitive subgroup D_4 of S_4 has three surjections to C_2, the sign character h_+, the "canonical character" h_c, and their product h_{+c}. Here h_c is distinguished from the others by having a cyclic kernel.

Finally the groups with product closure $S_2 S_2 S_2$ also require a special

comment. Explicitly the three proper subgroups are

$$S_2S_2^+S_2 = \{\mathrm{Id}, (12), (34)(56), (12)(34)(56)\}$$
$$(S_2S_2S_2)^+ = \{\mathrm{Id}, (12)(34), (12)(56), (34)(56)\}$$
$$S_2^+S_2^+S_2 = \{\mathrm{Id}, (12)(34)(56)\}.$$

Only the middle of these groups doesn't fit nicely in our set-up, being $S_2S_2S_2 \cap A_6$.

The 40 intransitive subgroups of S_6

1	S_1				
2	S_2				
3	S_3	A_3			
4	S_4	A_4	D_4	C_4	V
5	S_5	A_5	F_5	D_5	C_5
22	S_2S_2 $S_2^+S_2$				
32	S_3S_2 $S_3^+S_2$	A_3S_2			
33	S_3S_3 $S_3^+S_3$ $S_3^\Delta S_3$	S_3A_3	A_3A_3 $A_3^\Delta A_3$		
42	S_4S_2 $S_4^+S_2$	A_4S_2	D_4S_2 $D_4^+S_2$ $D_4^cS_2$ $D_4^{c+}S_2$	C_4S_2 $C_4^+S_2$	VS_2 V_hS_2
222	$S_2S_2S_2$ $S_2S_2^+S_2$ $(S_2S_2S_2)^+$ $S_2^+S_2^+S_2$				

The 16 *transitive subgroups of* S_6. The transitive subgroups of S_6 fall naturally into four families, according to whether the G-set

$\{1,2,3,4,5,6\}$ has G-quotient sets of order 2 or 3. The primitive case—no such quotients—breaks up into two subcases, associated to the groups S_6 and $PGL_2(\mathbf{F}_5)$.

Primitive		Quadratic quotient set only		Cubic quotient set only		Quadratic and Cubic quotients	
S_6		$C_3^2.D_4$		$S_2 \wr S_3$		D_6	
A_6	ε_6	$C_3^2.C_4$	ε_6	$S_2 \wr^+ S_3$	ε_6	$S_{3\text{gal}}$	ε_6
$PGL_2(\mathbf{F}_5)$		$C_3^2.V$	$\varepsilon_6\varepsilon_2$	$V.S_3$	$\varepsilon_3\varepsilon_6$	C_6	ε_3
$PSL_2(\mathbf{F}_5)$	ε_6	$C_3^2.C_2$	—	$S_2 \wr A_3$	ε_3		
				$S_2 \wr^+ A_3$	$\varepsilon_6, \varepsilon_3, \varepsilon_6\varepsilon_3$		

In each of the five boxes above, the top group is the largest group in its subcase. On this group are defined quadratic characters $\varepsilon_6, \varepsilon_3$ and/or ε_2, the sign characters of the indicated degree.

Nine of the remaining eleven groups have index two in the associated ambient group. These are kernels of quadratic characters as indicated. The group here denoted $S_2 \wr^+ A_3$ has index four in $S_2 \wr S_3$, being the intersection of the kernels of ε_3 and ε_6. The lone group not fitting in this system is $C_3^2.C_2$ which is a nonnormal subgroup of index four in its ambient group $C_3^2.D_4$.

The ambient group in the quadratic-quotient-set-only box would normally be written as a wreath product $S_3 \wr S_2$. We use the notation $C_3^2.D_4$ instead, just so the notations for the various groups don't look too similar. Similarly, a notation for D_6 more appropriate to the present setting would be $S_3 \times S_2$.

3. Sextic twinning. Here we first define a canonical operation which associates to a six element set X its twin X^t. This exceptional operation can be viewed as analogous to taking the dual of a finite-dimensional F-vector space, $V \mapsto V^t$. Then we continue the discussion, reinterpreting twinning as coming from the exceptional outer automorphism of S_6. This is analogous to vector space duality coming from the natural outer automorphism of $GL_n(F)$, represented by the involution "inverse-transpose." Finally we present Girstmair's explicit twinning operator on algebras [**4**] and a simpler twinning operator which applies in a special case.

Set-theoretic twinning. Let X be a set with six elements. A *duad* of X is a subset of order 2. So the set $S_2(X)$ of duads has 15 elements. A *syntheme* of X is a set of three nonoverlapping duads. So there are 15 synthemes. A *total* of X is a set of five synthemes whose constituent 15 duads are all distinct. Not so obviously there are six totals. We denote the set of totals by X^t. Each pair of totals has exactly one syntheme in common so that the set of synthemes is naturally identified with $S_2(X^t)$.

Many aspects of this construction become clearer when reformulated in group-theoretic terms. Let $G = \mathrm{Sym}\,(X)$. Then there are canonical bijections

$$\begin{aligned} X &\xrightarrow{\sim} \{\text{120-element subgroups of } G \text{ with fixed points}\} \\ x &\longmapsto G_x \end{aligned}$$

$$\begin{aligned} S_2(X) &\xrightarrow{\sim} \{\text{Odd involutions in } G \text{ with fixed points}\} \\ \{a,b\} &\longmapsto (ab) \end{aligned}$$

$$\begin{aligned} S_2(X^t) &\xrightarrow{\sim} \{\text{Odd involutions in } G \text{ without fixed points}\} \\ \{\{a,b\},\{c,d\},\{e,f\}\} &\longmapsto (ab)(cd)(ef) \end{aligned}$$

$$\begin{aligned} X^t &\xrightarrow{\sim} \{\text{120-element subgroups of } G \text{ without fixed points}\} \\ y &\longmapsto G_y. \end{aligned}$$

In particular, there is clearly a) no natural isomorphism $X \mapsto X^t$ and b) a natural isomorphism $X \mapsto X^{tt}$.

Take $X = \{1,2,3,4,5,6\}$. The six columns of the symmetric matrix below explicitly give the six totals of X, thereby giving an identification $X^t = \{A,B,C,D,E,F\}$. The entries of this matrix can be interpreted as equalities in $\mathrm{Sym}\,(X) = \mathrm{Sym}\,(X^t)$; for example, at the (A,B) place is indicated the equality $(AB) = (15)(23)(46)$.

	A	B	C	D	E	F
A		15,23,46	14,26,35	13,24,56	12,36,45	16,25,34
B	15,23,46		12,34,56	14,25,36	16,24,35	13,26,45
C	14,26,35	12,34,56		16,23,45	13,25,46	15,24,36
D	13,24,56	14,25,36	16,23,45		15,26,34	12,35,46
E	12,36,45	16,24,35	13,25,46	15,26,34		14,23,56
F	16,25,34	13,26,45	15,24,36	12,35,46	14,23,56	

Here the last column was determined first. It is the total labeled F and stabilized by $PGL_2(\mathbf{F}_5)$ where one uses the alternative notation $5 = 0$, $6 = \infty$. The remaining entries were determined by the simple formula

$$(UV) = (FU)(FV)(FU)$$

in the symmetric group $\mathrm{Sym}\,(\{F, U, V\}) \subset \mathrm{Sym}\,(\{A, B, C, D, E, F\})$.

As a sample trivial calculation, we show how to use the above chart to express the action of (123) on X^t. The signs "$\mapsto$" below all indicate conjugation by (123), i.e., $g \mapsto (123)g(321)$.

$$\begin{aligned}
(AF) = (16)(25)(34) &\longmapsto (26)(35)(14) = (CA)\\
(BF) = (13)(26)(45) &\longmapsto (21)(36)(45) = (EA)\\
&\text{so } F \longmapsto A, A \longmapsto C, B \longmapsto E\\
(CF) = (15)(24)(36) &\longmapsto (25)(34)(16) = (FA)\\
&\text{so } C \longmapsto F\\
(DF) = (12)(35)(46) &\longmapsto (23)(15)(46) = (BA)\\
&\text{so } D \longmapsto B\\
(EF) = (14)(23)(56) &\longmapsto (24)(31)(56) = (DA)\\
&\text{so } E \longmapsto D.
\end{aligned}$$

Hence $(123) = (ACF)(BED)$.

The outer automorphism. An element σ of $G = \mathrm{Sym}\,(X)$ gives rise to both a permutation σ of X and a permutation σ^t of X^t. Let τ be a bijection $X \xrightarrow{\sim} X^t$. Then $\sigma^\tau = \tau^{-1}\sigma^t\tau$ is a permutation of X. The map $\sigma \mapsto \sigma^\tau$ is an automorphism representing the outer automorphism

t. The most important fact about t is that its action on $S_6^\natural$ switches three pairs of partitions

$$\begin{aligned} 31^3 &\longleftrightarrow 33 \\ 21^4 &\longleftrightarrow 2^3 \\ 6 &\longleftrightarrow 321 \end{aligned}$$

and fixes the remaining five partitions. The classical duad/syntheme treatment of twinning is based on the switch $21^4 \leftrightarrow 2^3$ while the equality $(123) = (ACF)(BED)$ illustrates the switch $31^3 \leftrightarrow 33$.

A representing automorphism. For computations it is convenient to pick one of the 720 automorphisms of $G = S_6$ representing t. Here we pick such a τ and explain its attractive features.

Firstly, only 36 of the 720 choices for τ are involutions (in [**2**] they form the class $2D$ in the group $S_6.2$). These are indexed by pairs (x, y) with $x \in X$ and $y \in X^t$. The associated bijection is partially defined by $\tau_{x,y}(x) = y$. The definition is completed by the following construction. Given $x_1 \neq x$ there is one syntheme in the total y that contains the 2-cycle (xx_1); this syntheme is contained in just one other total y_1. The rest of the definition is $\tau_{x,y}(x_1) = y_1$.

Secondly, we have carefully chosen things above so that the alphabetical order bijection $1 \mapsto A, \ldots, 6 \longmapsto F$ is one of these involutive automorphisms, namely, $\tau_{6,F}$. Let $G_{x,y} = G_x \cap G_y$. As (x, y) runs over the 36 possibilities, $G_{x,y}$ runs over the 36 subgroups of G having order 20. The fixed point set of the automorphism $\tau_{x,y}$ is exactly $G_{x,y}$. Exactly for $g \in G_{x,y}$ are the two notations for g the same, via $\tau_{x,y}$. For example, our choice of $\tau_{6,F} = \tau_{\infty,F}$ identifies $G_{x,y}$ with the group of affine transformations of $\mathbf{F}_5$. As three examples, one has

$$\begin{aligned} \text{“plus 1”} &= (12340)(\infty) = (ABCDE)(F) \\ \text{“times 2”} &= (1243)(0)(\infty) = (ABDC)(E)(F) \\ \text{“times 4”} &= (14)(23)(0)(\infty) = (AD)(BC)(E)(F). \end{aligned}$$

These examples illustrate that the conjugacy classes 51, 411 and 2211 are each fixed by the twinning operation.

Girstmair's resolvent. The group $G = S_6$ acts on the ring $R = \mathbf{Z}[x_1, \ldots, x_6]$ via $\sigma(x_i) = x_{\sigma(i)}$. Define elements $a_1, \ldots, a_6$ in R by the

formula

$$\prod_{i=1}^{6}(z-x_i) = z^6 + a_1 z^5 + \cdots + a_5 z + a_6.$$

Then, by the theory of symmetric functions, the ring R^G of invariants is the polynomial ring $\mathbf{Z}[a_1, \ldots, a_6]$.

Consider the 15-element set of synthemes. To each syntheme ab, cd, ef let's associate two elements of R, namely,

$$\begin{aligned} p'_{ab,cd,ef} &= x_a x_b + x_c x_d + x_e x_f \\ p_{ab,cd,ef} &= x_1^2 x_b^2 (x_c x_d + x_e x_f) + x_c^2 x_d^2 (x_a x_b + x_e x_f) \\ &\quad + x_e^2 x_f^2 (x_a x_b + x_c x_d). \end{aligned}$$

Thus, both p' and p give G-equivariant maps from $S_2(X^t)$ into R; they are both clearly injective.

To a total J, let's also associate two elements of R, namely,

$$y'_J = \sum_{s \in J} p'_s, \qquad y_J = \sum_{s \in J} p_s.$$

Here in each case the sum is over the five synthemes s in the total J. Again both y and y' give G-equivariant maps from X^t into R. But here y' is a constant map while y is injective. We therefore drop y' from consideration; it was included only for comparison.

The sextic polynomial

$$R = \prod_{J \in X^t} (z - y_J)$$

is invariant under S_n. It therefore can be written as

$$R(a_1, a_2, \ldots, a_5, a_6; z) = \sum_{j=0}^{6} b_j(a_1, a_2, a_3, a_4, a_5, a_6) z^j.$$

For example a special case emphasized by Girstmair is

$$\begin{aligned} R(0,0,0,0,a_5,a_6;z) = z^6 &+ 18a_6 z^5 - 135a_6^2 z^4 - 3240a_6^3 z^3 \\ &+ (93312a_6^5 + 3125a_5^6)z \\ &+ (40625a_5^6 a_6 - 186624a_6^6). \end{aligned}$$

Also given there (pp. 794–796) is the essentially general case where only a_1 is set equal to zero. Then the polynomials $b_1, \dots, b_6$ have 2, 9, 23, 45, 86, 146 terms, respectively.

Girstmair's resolvent is an explicit formula for the twinning operation. Namely, suppose K is an algebra defined by a sextic separable polynomial

$$f(z) = z^6 + a_1 z^5 + \cdots + a_6$$

over a ground field F. Suppose also that the polynomial

$$f^t(z) = z^6 + b_1(a_1, \dots, a_6)z^5 + \cdots + b_6(a_1, \dots, a_6)$$

is separable. Then the dual algebra is defined by f^t. This twinning operation provides a common complicated generalization of many much simpler classical constructions. For example, suppose $f(z)$ factors as $f_3(z)z(z-1)(z-2)$ with the cubic field $K_3 = F[z]/f_3(z)$ having Galois group S_3. Then $f^t(z)$, if separable, is irreducible, defining a Galois-closed field associated to K_3.

Of course one does not have twinning at the level of polynomials; rather the roots of f^{tt} are homogeneous functions of the roots of f of degree $6^2 = 36$. For the $a_i \in \mathbf{Z}$ one can work numerically with the complex roots $x_1, \dots$ of f and the complex roots $y_A(x_1, \dots, x_6), \dots$ of f^t, thereby bypassing Girstmair's rather unwieldy formula.

Separability. The separability of f does not in general guarantee the separability of f^t. For example, note that the five synthemes of B are switched with the five synthemes of C via the involution $(BC) = (12)(34)(56)$. Suppose the roots of f in some $\overline{F}$ satisfy the algebraic relations

$$x_1 = -x_2, \qquad x_3 = -x_4, \qquad x_5 = -x_6,$$

forcing the Galois group of K to be in $S_2 \wr S_3$. Then, for all $J \in \{A, D, E, F\}$, one has equality

$$p_{JB}(x_1, \dots, x_6) = p_{JC}(x_1, \dots, x_6)$$

in $\overline{F}$. Accordingly, two roots of f^t coincide,

$$y_B(x_1, \dots, x_6) = y_C(x_1, \dots, x_6),$$

giving the nonseparability of f^t.

The situation however is not too bad. Firstly, from the general theory of resolvents, one knows that a generic choice of f defining K gives a separable f^t. Hence, if F is infinite, an f can always be chosen so that f^t is separable. Secondly, Girstmair proves [**5**, Theorem 6] that if 5 divides the order of $\mathrm{Gal}(K)$ then any choice of f gives a separable f^t.

Mini-twinning. When a six-element set X is given an appropriate extra structure, one can sometimes use this structure to give a simpler description of the twin set X^t. Here we just give one example.

Suppose quite generally that Y and Z are nonempty finite sets with $m := |Y|/|Z|$ integral. Let $S(X,Y)$ be the set of fibrations from Y to Z, i.e., the set of surjections with all fibers having m elements. The symmetric groups $\mathrm{Sym}\,(Y)$ and $\mathrm{Sym}\,(Z)$ act by composition on $S(Y,Z)$ on the left and right, respectively.

This general set-theoretic situation is of theoretical importance in Galois theory. Let $K = F[x]/f(x)$ have root set Y and $L = F[x]/g(x)$ have root set Z. Corresponding to the $\mathrm{Gal}(\overline{F}/F)$-set $S(Y,Z)$ is an algebra $I(L,K)$. The trivial factors of $I(L,K)$ are in bijection with the embeddings $L \hookrightarrow K$.

Let $\{\alpha_y\}_{y\in Y}$ and $\{\beta_z\}_{z\in Z}$ be the roots of f and g, respectively. Then

$$f(x) = \prod_{\phi\in S(Y;Z)} \left(x - \sum_{y\in Y} \alpha_y \beta_{\phi(y)} \right) \in F[x],$$

if separable, defines the algebra $I(L,K)$.

Now take $|Y| = |Z| = 3$ and put $X = Y \coprod Z$. Then the set $S(Y,Z)$ is naturally identified with X^t. Namely to an isomorphism $\phi : Y \to Z$ associate the total

$$\begin{aligned} T_\phi = \{&\Gamma_{\psi_1}, \Gamma_{\psi_2}, \\ &\{\{y_1, \phi(y_1)\}, \{y_2, y_3\}, \{\phi(y_2), \phi(y_3)\}\}, \\ &\{\{y_2, \phi(y_2)\}, \{y_3, y_1\}, \{\phi(y_3), \phi(y_1)\}\}, \\ &\{\{y_3, \phi(y_3)\}, \{y_1, y_2\}, \{\phi(y_1), \phi(y_2)\}\}\}. \end{aligned}$$

Here ψ_1 and ψ_2 are the two isomorphisms ψ from Y to Z which are different from ϕ but such that $\psi^{-1} \circ \phi$ is an even permutation

of Y; Γ_{ψ_1} and Γ_{ψ_2} are their graphs, considered as synthemes. Also $Y = \{y_1, y_2, y_3\}$. Applying the theory of symmetric functions we get a "mini-twinning" formula.

Proposition 1. *Suppose*

$$f(x) = (x^3 + a_2x + a_3)(x^3 + b_2x + b_3)$$

defines the sextic algebra K. Then

$$\begin{aligned} f^\tau(x) = x^6 - 6a_2b_2x^4 - 27a_3b_3x^3 + 9a_2^2b_2^2x^2 \\ + 81a_2a_3b_2b_3x - (4a_2^3b_2^3 + 27a_3^2b_2^3 + 27a_2^3b_3^2), \end{aligned}$$

when separable, defines the twin algebra K^t.

In practice one can also use this formula for K with $\mathrm{Gal}(K) \subseteq C_3^2.D_4$. Namely let $K = F[x]/f(x)$ with $f(x)$ factoring as indicated over a quadratic extension F' of F. Then the polynomial $f^\tau(x)$ is still in $F[x]$ and still defines K^t.

4. Conjugacy classes and characters. When one is studying an algebra extension K/F with Galois group $G = \mathrm{Gal}(K)$, it is useful to have the character table of G at hand. Since we are considering 56 situations at once we will just present partial information about each situation, so that the situations can be easily compared.

So that the tables fit on a page we divide the 56 groups into two classes. The first class consists of the 28 groups G such that at least one of G and G^t is transitive. This class is discussed at some length in [**3**, especially p. 298]. The second class consists of the remaining 28 groups. For groups of the first class, information about conjugacy classes is presented in the first table, and information about characters in the second table. Our first table is essentially a considerably more detailed version of the sextic table in [**1**]. The groups of the second class tend to be smaller; so the corresponding information is put all on the third table.

Table 1. A given row of the first table goes as follows. The first entry is the order $|G|$. The second entry G is a transitive subgroup of S_6.

TABLE 1. Conjugacy classes in G and G^t with G transitive.

$\|G\|$	G	G^t	A^t	1^6	2^21^2	$31^3 \leftrightarrow 3^2$		51	42	$21^4 \leftrightarrow 2^3$		41^2	$321 \leftrightarrow 6$	
Primitive														
720	S_6			1	45	40	40	144	90	15	15	90	120	120
360	A_6			1	45	40	40	*72,72*	90					
120	$PGL_2(\mathbf{F}_5)$	S_5		1	15		20	24			10	30		20
60	$PSL_2(\mathbf{F}_5)$	A_5		1	15		20	*12,12*						
Contains cubic														
48	$S_2 \wr S_3$	S_4S_2	S_2	1	3,6		8		6	3	1,6	6		8
24	$S_2 \wr^+ S_3$	$S_4^+S_2$	S_2	1	3,6		8		6					
24	$V.S_3$	S_4	S_2	1	3		8				6	6		
24	$S_2 \wr A_3$	A_4S_2	S_2	1	3		**4,4**			3	1			**4,4**
12	$S_2 \wr^+ A_3$	A_4	S_2	1	3		**4,4**							
Contains quadratic														
72	$C_3^2.D_4$			1	9	4	4		18	6	6		12	12
36	$C_3^2.C_4$			1	9	4	4		**9,9**					
36	$C_3^2.V$	S_3S_3		1	9	4	2,2				3,3			6,6
18	$C_3^2.S_2$	S_3A_3	A_3	1		**2,2**	2,**1,1**				3			**3,3**
Contains both														
12	D_6	S_3S_2	S_2	1	3		2				1,3			2
6	$S_{3\text{gal}}$	S_3	S_3	1			2				3			
6	C_6	A_3S_2	A_3S_2	1			**1,1**				1			**1,1**

The third entry is blank if and only if $G = G^t$ and G^t otherwise; in this latter case G^t is always intransitive.

Let A be the centralizer of G and A^t the centralizer of G^t. The fourth entry gives A^t when not the trivial group. Here we print A^t rather than A because it is often completely obvious how G^t and A^t commute with one another, and sometimes not quite so obvious how G has a nontrivial centralizer.

The printed numbers in the last 11 columns give the masses $\mu(c)$ of the conjugacy classes of $c \in G^\natural$. If c induces the partition λ of 6, then $\mu(c)$ is printed in the λ column.

Suppose any representative g of c has order e. Then for $i \in \mathbf{Z}/e$ the element g^i represents a well-defined class c^i. If, for all $i \in (\mathbf{Z}/e)^\times$ one has $c = c^i$, then the class c is called rational; then $\mu(c)$ is printed in plain type. If $c^{-1} = c$, then the class is called real; if c is real but nonrational, then $\mu(c)$ is printed in italics. The remaining classes c are nonreal; $\mu(c)$ is printed in bold face.

Frobenius elements. An important use of tables such as the one above is the following. Suppose, for example, $F = \mathbf{Q}$ and K is given by a sextic polynomial f with discriminant D and Galois group $G = \mathrm{Gal}(K)$. Then for all primes p not dividing D there is a Frobenius class $\mathrm{Fr}_p \in \mathrm{Gal}(K)^\natural$; the Cebotarev density theorem says that they are equidistributed according to the indicated masses. As an element of $S_n^\natural$, Fr_p is just the factorization pattern of f modulo p.

Suppose for example that one has computed three Frobenius elements in $S_6^\natural$ finding them to be 42, 411 and 6. Then the Galois group is necessarily $S_2 \wr S_3$ or S_6. Suppose f^t has nonzero discriminant D^t and moreover factors nontrivially, $f^t = f_4^t f_2^t$. Then the factors must have the indicated degrees and $G = S_2 \wr S_3$.

Suppose still that $G = S_2 \wr S_3$. Then computation with f alone lets one see Frobenius classes only in an eight-element set. Computation with $f_4^t f_2^t$ lets one see Frobenius classes where they really live, the 10 element set $\{1111, 22, 31, 211, 4\} \times \{11, 2\}$.

In general, let $G^{\natural\mathrm{rat}}$ be the quotient of $G^\natural$ by the power action of $\mathbf{Z}/|G|^\times$. Then the use of resolvent polynomials like above allows one to compute Galois groups always, but Frobenius elements only in $G^{\natural\mathrm{rat}}$.

In our current special case $F = \mathbf{Q}$ one can use cyclotomic reciprocity to resolve some of the remaining ambiguities. Namely, G^{ab} is identified with a quotient group of $(\mathbf{Z}/D)^{\times}$ such that $\mathrm{Fr}_p = p$. In the cases covered by Table 1 the map $G^{\natural} \to G^{\natural\mathrm{rat}} \times G^{\mathrm{ab}}$ is injective except in the cases $G = A_5$, $PSL_2(\mathbf{F}_5)$, and A_6, where the unique ambiguity remains. Once again, a main purpose in our presenting of Table 1 is to show at a glance how all these well-known generalities apply in the current particular case.

Table 2. The next table gives for each of the 16 transitive groups G, the degree of its irreducible characters. The first number printed is always 1; this corresponds to the trivial character. If G is an odd group, then there is a second distinguished one-dimensional character, the parity character ε.

For G one of the groups S_6, $PGL_2(\mathbf{F}_5)$ or $C_3^2.D_4$ the 1 corresponding to ε is printed in the first column of character degrees. Two characters are printed in the same column if and only if they differ by multiplication by ε. The restrictions of χ and $\chi\varepsilon$ to the even subgroup A_6, $PSL_2(\mathbf{F}_5)$ or $C_3^2.C_4$ agree. This restriction is either irreducible or the sum of two irreducible characters, as indicated by the entry for the even subgroup in the same column.

For G^t one of the six groups with a canonical product structure, the order of the printed character degrees respects this structure. Thus, for example, the entry for $G^t = S_3S_3$ is better displayed

$$\begin{array}{ccc} 1 & 1 & \underline{2} \\ 1 & \overline{1} & 2 \\ \underline{2} & 2 & \overline{4} \end{array}$$

For the groups with $G^t = HA_3$ the entries in a given column correspond in order to χ, $\chi\phi$ and $\chi\bar{\phi}$ for $X \in \hat{H}$ and $\hat{A}_3 = \{1, \phi, \bar{\phi}\}$. Similarly for the groups with $G^t = HS_2$, the entries in a given column correspond to χ and $\chi\phi$ with $X \in \hat{H}$ and $\hat{S}_2 = \{1, \phi\}$.

Characters taking only rational values have their degrees printed in plain type. Characters taking only real but some nonrational values have their degrees printed in italics. Characters taking some nonreal values have their degrees printed in bold type. The familiar duality between characters and conjugacy classes says in particular that

$|G_*^\natural| = |\hat{G}_*|$ for $*$ running over "rational," "*real-but-nonrational*," and "**nonreal**." These equalities are all seen easily when one compares Tables 1 and 2. Similarly, the Frobenius-Schur theorem says in particular that the sum of the degrees of the real characters is the number of involutions in G; we're using that all real characters for the groups here are orthogonal rather than symplectic. Again this can be checked case-by-case by comparing Tables 1 and 2.

TABLE 2. Character degrees of G and G^t with G transitive.

$\lvert G\rvert$	G	G^t	Degrees					
720	S_6		1,1	$\overline{5}, 5$	$\underline{5}, 5$	9,9	10,10	16
360	A_6		1	$\overline{5}$	$\underline{5}$	9	10	*8,8*
120	$PGL_2(\mathbf{F}_5)$	S_5	1,1	$4, \underline{4}$	$5, \overline{5}$	6		
60	$PSL_2(\mathbf{F}_5)$	A_5	1	$\underline{4}$	$\overline{5}$	3,3		
48	$S_2 \wr S_3$	S_4S_2	$1, \underline{1}$	1,1	$\overline{2}, 2$	$\underline{3}, 3$	$3, \overline{3}$	
24	$S_2 \wr^+ S_3$	$S_4^+S_2$	1	$\underline{1}$	$\overline{2}$	$\underline{3}$	$\overline{3}$	
24	$S_2 \wr^\varepsilon S_3$	S_4	1	1	$\overline{2}$	$\underline{3}$	$\overline{3}$	
24	$S^2 \wr A_3$	A_4S_2	$1, \underline{1}$	$\overline{\mathbf{1}}, \mathbf{1}$	$\overline{\mathbf{1}}, \mathbf{1}$	$\underline{3}, \overline{3}$		
12	$S_2 \wr^+ A_3$	A_4	1	$\overline{\mathbf{1}}$	$\overline{\mathbf{1}}$	$\underline{\overline{3}}$		
72	$C_3^2.D_4$		1,1	$\overline{1}, \underline{1}$	2	$\overline{4}, 4$	$\underline{4}, 4$	
36	$C_3^2.C_4$		1	$\underline{\overline{1}}$	$\mathbf{1}, \mathbf{1}$	$\overline{4}$	$\underline{4}$	
36	$C_3^2.V$	S_3S_3	$1, 1, \underline{2}$	$1, \overline{1}, 2$	$\underline{2}, 2, \overline{4}$			
18	$C_3^2.S_2$	S_3A_3	$1, \underline{\mathbf{1}}, \underline{\mathbf{1}}$	$\overline{1}, \mathbf{1}, \mathbf{1}$	$2, \overline{\mathbf{2}}, \overline{\mathbf{2}}$			
12	D_6	S_3S_2	$1, \underline{\overline{1}}$	1,1	$\underline{\overline{2}}, \overline{2}$			
6	C_6	A_3S_2	$1, \underline{\overline{\mathbf{1}}}, \underline{\overline{\mathbf{1}}}$	$\underline{\overline{1}}, \overline{\mathbf{1}}, \overline{\mathbf{1}}$				
6	$S_{3\text{gal}}$	$S_3^+S_2$	1	$\underline{\overline{1}}$	$\underline{\overline{\overline{2}}}$			

The final information contained in Table 2 below is the following. Consider the given degree 6 permutation character ϕ of G and the twin character ϕ^t. Each of these decomposes as a sum of irreducible linear characters. The nonunital constituents of ϕ are indicated by overbars and the nonunital constituents of ϕ^t by underbars. Thus, for example,

TABLE 3. Conjugacy classes and character degrees of G and G^t with both groups intransitive.

$\lvert G\rvert$	G	G^t	A	1^6	2^21^2	$31^3 \leftrightarrow 3^2$	51	42	$21^4 \leftrightarrow 2^3$	41^2	Degrees
20	F_5			1	5		4			**55**	$1\,1\,\mathbf{1}\,\mathbf{1}\,\underline{4}$
10	D_5			1	5		*22*				$1\,1\,\underline{\overline{22}}$
5	C_5		C_5	1			**1111**				$1\,\underline{\mathbf{1}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}}$
16	D_4S_2		$S_2^+S_2S_2$	1	122			2	12	12 2	$1\,1\,1\,1\,\underline{1}\,\underline{1}\,\overline{1}\,\overline{1}\,\underline{2}\,\overline{2}$
8	$D_4^cS_2$	D_4	$S_2^+S_2S_2$	1	12				2	2	$1\,\underline{1}\,\overline{1}\,\underline{1}\,\underline{2}$
8	$D_4^+S_2$		$S_2^+S_2S_2$	1	122			2			$1\,1\,\underline{\overline{1}}\,\underline{\overline{1}}\,\underline{2}$
8	$D_4^{+c}S_2$		$S_2^+S_2S_2$	1	1				2	2 2	$1\,1\,\underline{\overline{1}\,\overline{2}}$
8	C_4S_2		C_4S_2	1	1			**11**	1	1 **11**	$1\,\underline{1}\,\underline{\overline{1}}\,\underline{\overline{1}}\,\underline{\overline{1}}\,\underline{\mathbf{1}\,\mathbf{1}}$
4	$C_4^+S_2$		C_4S_2	1	1			**11**			$1\,\underline{\overline{\mathbf{1}}}\,\underline{\mathbf{1}\,\mathbf{1}}$
4	C_4		C_4S_2	1	1					**11**	$1\,\underline{\overline{\mathbf{1}\,\mathbf{1}}}$
18	$S_3^+S_3$			1	9	22 22					$1\,1\,\underline{\overline{2}\,\overline{2}}\,\underline{2}\,\underline{2}$
9	A_3A_3		A_3A_3	1		**1111 1111**					$1\,\underline{\overline{\mathbf{1}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}}}\,\underline{\mathbf{1}\,\mathbf{1}\,\mathbf{1}\,\mathbf{1}}$
6	$S_3^\Delta S_3$	$S_3^+S_2$	S_2	1	3	2					$1\,\underline{\overline{1}}\,\underline{\overline{2}}$
3	$A_3^\Delta A_3$	A_3	A_3S_3	1		**11**					$1\,\underline{\overline{\mathbf{1}}}\,\underline{\overline{\mathbf{1}}}$
8	VS_2	$S_2S_2S_2$	$S_2S_2S_2$	1	111			generic	1	111	$1\,\underline{\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}}\,\underline{1}\,\underline{1}\,\underline{1}$
4	V	$(S_2S_2S_2)^+$	$S_2S_2S_2$	1	111			$abc{=}1$			$1\,\underline{\overline{1}\,\overline{1}\,\overline{1}}$
4	$V^\varepsilon S_2$	S_2S_2	$S_2S_2S_2$	1	1			$c{=}1$		11	$1\,\underline{\overline{1}}\,\underline{\overline{1}}\,\underline{1}$
4	$S_2^+S_2S_2$		$S_2S_2S_2$	1	1			$ab{=}1$	1	1	$1\,\underline{\overline{1}}\,\underline{\overline{1}}\,\underline{\overline{1}}$
2	$S_2^+S_2$		D_4S_2	1	1			$ab{=}c{=}1$			$1\,\underline{\overline{\mathbf{1}}}\,\underline{\overline{\mathbf{1}}}$
2	$S_2^+S_2^+S_2$	S_2	$S_2 \wr S_3$	1				$a{=}b{=}c$		1	$1\,\underline{\overline{\mathbf{1}}}\,\underline{\overline{\mathbf{1}}}$
1	(Identity)		S_6	1				$a{=}b{=}c{=}1$			1

in the case $G^t = S_3S_3$, one has

$$\phi = 1 + \varepsilon_1\varepsilon_2 + \chi_1\chi_2$$
$$\phi^t = (1 + \chi_1) + (1 + \chi_2).$$

Here χ_1 and χ_2 are the two-dimensional characters of the factor S_3's and ε_1 and ε_2 are their respective determinants.

Table 3. The next table presents its information in a way similar to Tables 1 and 2. It may at first seem excessive to treat these quite small groups in such detail. Recall, however, that the principal application we have in mind is to Galois groups G of sextic number fields and their decomposition groups D_p. In this application G, being assumed transitive, certainly is covered by Tables 1 and 2; but each D_p, being typically very small, usually is one of the groups of Table 3.

From a twin pair of groups, we take G to be the subgroup with fewer orbits on $X = \{1, 2, 3, 4, 5, 6\}$, in the spirit of Table 1; the only tie is $(G, G^t) = (V, (S_2S_2S_2)^+)$, each group having three orbits. Otherwise, the format requires no further explanation.

The last seven lines of Table 3 can be immediately translated into algebra-theoretic terms. For simplicity, take $\mathrm{char}\,(F) \neq 2$. For $a, b \in F^\times$ put

$$F_a = F[x]/(x^2 - a) \qquad (= F(\sqrt{a}))$$
$$F_{a,b,ab} = F[x, y]/(x^2 - a, y^2 - b) \quad (= F(\sqrt{a}, \sqrt{b})).$$

The algebra F_a depends only on $a \in F^\times/F^{\times 2}$. Similarly, the algebra $F_{a,b,c}$ depends only on $a, b, c \in F^\times/F^{\times 2}$, satisfying $abc = 1 \in F^\times/F^{\times 2}$. The parenthetical definitions are also correct, provided one understands them in the sense of algebras, e.g., $F(\sqrt{1}) \cong F \times F$. The last seven lines all correspond to algebras of the form

$$K = F_{ab,bc,ac} \times F_{abc}$$
$$K^t = F_a \times F_b \times F_c.$$

The first of these lines is the generic case of this situation; it is followed by the specializations indicated on the table.

Here are some supplementary details about characters for the second block of groups. Let $K = K_4 \times K_2$ be a sextic algebra. Here K_4 is a quartic field with a unique quadratic subfield L_2. On the other hand, K_2 is allowed to be either a field or $F \times F$. Let $\varepsilon_4, \varepsilon_4\varepsilon_c$ and ε_2 be the discriminant characters of K_4, L_2 and K_2, respectively. Then the sextic permutation character of G has the form

$$\phi = (1 + \chi + \varepsilon_4\varepsilon_c) + (1 + \varepsilon_2).$$

Here the two-dimensional character χ is irreducible in the cases involving D_4, reducible in the cases involving C_4; in both cases its determinant is ε_c. The twin algebra has the same form: $K^t = K_4^t \times K_2^t$, $L_2^t \subset K_4^t$. Its characters are given by

$$\begin{aligned} \varepsilon_4^t &= \varepsilon_4\varepsilon_c, & \varepsilon_2^t &= \varepsilon_2\varepsilon_c \\ \varepsilon_c^t &= \varepsilon_c, & \chi^t &= \chi\varepsilon_2. \end{aligned}$$

We have given this situation special mention because the 2-adic sextic algebras appearing in [**7**] very often have this form.

From conjugacy classes to characters. The next table illustrates how one goes from the printed conjugacy class information to the printed over- and under-barring on the character degrees. Let ϕ be the standard degree six permutation character on S_6 and ϕ^t the other degree six permutation character. Their values are printed below. Consider as an example the last group $G = VS_2$ and its twin $G^t = S_2S_2S_2$. They induce the partitions 42 and 222 of six, respectively; hence, $\phi|G$ and $\phi^t|G$ have respectively two and three copies of the unital character 1. Accordingly, it is more useful to print $(\phi - 2)|G$ and $(\phi^t - 3)|G$. One sees

$$\int_{G^\natural} (\phi - 2)^2 \mu_{\text{Haar}} = 4$$

$$\int_{G^\natural} (\phi^t - 3)^2 \mu_{\text{Haar}} = 3$$

$$\int_{G^\natural} (\phi - 2)(\phi^t - 3) \mu_{\text{Haar}} = 0.$$

The first equation confirms the clear fact that $\phi - 2$ is the sum of four distinct characters; similarly the second shows that $\phi^t - 3$ is the sum of

TABLE 4. Identification of permutation characters in two sample cases.

		1^6	2^21^2	31^3	3^2	51	42	21^4	2^3	41^2	321	6
	ϕ	6	2	3	0	1	0	4	0	2	1	0
	ϕ^t	6	2	0	3	1	0	0	4	2	0	1
	$16\mu_{\text{Haar}}$	1	9	4	4							
$S_3^+S_3$	$\phi-2$	4	0	1	-2							
$S_3^+S_3$	ϕ^t-2	4	0	-2	1							
	$8\mu_{\text{Haar}}$	1	3					1	3			
VS_2	$\phi-2$	4	0					2	-2			
$S_2S_2S_2$	ϕ^t-3	3	-1					-3	1			

three distinct characters. The third gives the information one seeks: the first four characters are pairwise distinct from the last three. This corresponds to the printed information $1\overline{1111}\underline{111}$.

Similarly, the table above justifies the printed data $11\overline{22}\underline{22}$ for $G = S_3^+S_3$.

Self-twins. An algebra K is isomorphic to its twin K^t if and only if its Galois group $\mathrm{Gal}(K)$ is one of the seven groups printed in bold face below.

$\mathbf{F_5}$	$D_4^+S_2$	V	(**Identity**)
$\mathbf{D_5}$	$\mathbf{C_4^+S_2}$	$(S_2S_2S_2)^+$	
$\mathbf{C_5}$	$\mathbf{C_4}$	$\mathbf{S_2^+S_2}$	

One sees this as follows. First, a necessary condition for $K \cong K^t$ is that the characters ϕ and ϕ^t agree on $G = \mathrm{Gal}(K)$. This condition can be checked from the conjugacy class information above: $\phi = \phi^t$ if and only if $G^\natural$ maps into the partitions fixed by t, namely, $\{1^6, 2^21^2, 51, 42, 41^2\}$. Equally well, it can be checked from the character information: $\phi = \phi^t$ if and only if the overlining and underlining coincide. The ten groups printed above are exactly those satisfying $\phi = \phi^t$. Then inspecting these ten groups individually, one finds that in the bold-faced seven cases the permutation representations X and X^t underlying ϕ and ϕ^t are isomorphic.

Actually the more interesting situations are those with $\phi = \phi^t$ and $X \ncong X^t$. The first of these is the case $G = D_4^+ S_2$. Then

$$\phi = (1 + \chi + \varepsilon\varepsilon_c) + (1 + \varepsilon)$$
$$\phi^t = (1 + \chi + \varepsilon) + (1 + \varepsilon_c\varepsilon)$$

by the general $D_4 S_2$ twinning formulas given above, with $\varepsilon = \varepsilon_2 = \varepsilon_4$. Here in each case the two terms are the characters corresponding to the two orbits; the lack of agreement shows that the two permutation representations X and X^t of G are not isomorphic.

The second case with $\phi = \phi^t$ and $X \ncong X^t$ has $G = V$ and $G^t = (S_2 S_2 S_2)^+$. This is the first example of "Chebotarev ambiguity." Namely, V and $(S_2 S_2 S_2)^+$ are nonconjugate subgroups of S_6 inducing the same probability measure on $S_6^\natural$. The first examples from transitive subgroups of S_n appear in $n = 8$.

5. Geometric examples. Let $m \in \mathbf{Z}_{\geq 1}$. Let S be a set of m points in the complex projective line $\mathbf{P}^1 = \mathbf{C} \coprod \{\infty\}$. Let $T = \mathbf{P}^1 - S$ be the complement. For notational ease, we'll assume S is given in standard form

$$S = \{0, 1, s_2, s_3, \ldots, s_{m-3}, \infty\}$$

and moreover use the resulting ordering on S.

Choosing a base point $t \in T$ and loops γ_s around the s appropriately, one gets an identification

$$\pi_1(T, t) = \langle \sigma_0, \sigma_1, \ldots, \sigma_\infty | \sigma_0 \sigma_1 \cdots \sigma_\infty = e \rangle.$$

Thus $\pi_1(T, t)$ is a free group on any $m - 1$ of these generators; however, it is better to keep the points on the same footing and give the group by m generators and 1 relation as we've done.

If X is a degree n cover of T, then the fiber X_t is an n-element $\pi_1(T, t)$-set. In fact, this taking of fibers identifies the category of finite covers of T with the category of finite $\pi_1(T, t)$-sets.

If X is a degree n cover of T, then the action of σ_s on X_t determines a partition λ_s of n. This partition depends only on X and $s \in S$, not on our auxiliary choices so far.

Let $\overline{X}$ be the canonical smooth completion of X. So $\overline{X}$ has the structure of ramified cover of $\mathbf{P}^1$. Important numerical global invariants of $\overline{X}$ include the pairs (n_j, g_j) indexed by the set J of connected components of $\overline{X}$. Here n_j is the degree of $\overline{X}_j \to \mathbf{P}^1$ while g_j is the genus of $\overline{X}_j$. The local invariants λ_s do not determine these global invariants in general. They do, however, determine the Euler characteristic

$$\chi(\overline{X}) = \sum_j (2 - 2g_j)$$

via the Riemann-Hurwitz formula

$$\chi(\overline{X}) = n(2 - m) + \sum_s \text{ length } (\lambda_s).$$

Of course, in many cases, the λ_s force $|J| = 1$; in this case, the unique (n_j, g_j) is determined, being $(n, 1 - \chi(\overline{X})/2)$.

Let $\mathcal{C} = \mathcal{C}(\lambda_0, \lambda_1, \ldots, \lambda_\infty)$ denote the set of isomorphism classes of covers of T with ramification indices λ_s. Specializing the formula [**12**, Theorem 7.2.1] (by taking the ambient group G to be S_n), one gets a mass formula

$$\sum_{X \in \mathcal{C}} \frac{1}{|\text{Aut}(X)|} = \frac{|\lambda_0||\lambda_1| \cdots |\lambda_\infty|}{n!^2} \sum_{\chi \in \hat{S}_n} \frac{\chi(\lambda_0)\chi(\lambda_1) \cdots \chi(\lambda_\infty)}{\chi(1^n)^{m-2}}.$$

To describe the set $\mathcal{C}$ more explicitly, it is useful to have the complete list of subgroups of S_n. Suppose, for example, that $m = 3$. Suppose λ_0 is, for example, a given odd partition; suppose λ_1 and λ_∞ are allowed to vary over even and odd partitions, respectively. Let

$$\mathcal{C}(\lambda_0, +, -) = \coprod_{\lambda_1, \lambda_\infty} \mathcal{C}(\lambda_0, \lambda_1, \lambda_\infty).$$

Then one can describe $\mathcal{C}(\lambda_0, +, -)$ as follows. Choose $g_0 \in S_n$ representing λ_0. Let Cent $(g_0) \subseteq S_n$ be its centralizer. The group Cent (g_0) acts on A_n by conjugation; the orbits are naturally indexed by the set $\mathcal{C}(\lambda_0, +, -)$:

$$A_n = \coprod_{c \in \mathcal{C}(\lambda_0, +, -)} \text{Gen}_c.$$

Namely, let $g_1 \in \mathrm{Gen}_c$. Then the subgroup of S_n generated by the pair $\{g_0, g_1\}$ corresponds to a curve X indeed representing the class c. Also the associated Galois group, acting on the fiber X_t is just $\mathrm{Gal}(X,t) = \langle g_0, g_1 \rangle$, and $|\mathrm{Aut}(X)| = |\mathrm{Cent}\,(g_0)|/|\mathrm{Gen}_c|$.

In the following table we have carried out the above procedure for $n = 6$ and $\lambda_0 = 411$. Each box gives firstly the Euler characteristic computed from the above formula, whether or not $\mathcal{C}(411, \lambda_1, \lambda_\infty)$ is nonempty. Secondly, as X runs over representatives of $\mathcal{C}(411, \lambda_1, \lambda_\infty)$, the box gives the corresponding groups $\mathrm{Gal}(X)$.

TABLE 5. Classification of certain covers of the projective line.

$\lambda_1 \vert \lambda_\infty$	21^4	2^3	41^2	321	6
1^6	8	6	6 $.C_4$	6	4
$2^2 1^2$	6 $.D_4$	4 $.D_4^t$	4 $F_5F_5.\mathbf{C}_4$	4 $S_5.S_{42}$	2 $S_5^t.S_{42}^t$
31^3	6 $.S_4$	4	4 $S_5.\mathbf{S}_4$	4 S_5S_5	2 S_6
3^2	4	2 $.S_4^t$	2 $S_5^t.S_4^t$	2 S_6	0 $\mathbf{S}_5^t\mathbf{S}_5^t$
51	4 S_5	2 S_5^t	2 $\mathbf{S}_5\mathbf{S}_5^t\mathbf{F}_5\mathbf{F}_5$	2 $S_6S_6S_6S_6\mathbf{S}_5\mathbf{S}_5$	0 $\mathbf{S}_6\mathbf{S}_6\mathbf{S}_6\mathbf{S}_6\mathbf{S}_5^t\mathbf{S}_5^t$
42	4 $.C_{42}$	2 $.\mathbf{C}_{42}$	2 S_6S_6	2 $S_6S_6S_6S_6.\mathbf{S}_{42}$	0 $\mathbf{S}_6\mathbf{S}_6\mathbf{S}_6\mathbf{S}_6.\mathbf{S}_{42}^t$

Here we have adjusted our notations slightly so that every group is given by a single main letter together with sub/superscripts. The only changes are $S_{42} = S_4S_2$ and $C_{42} = C_4S_2$. The next four paragraphs explain how the above table illustrates various general phenomena.

Mass formula. We have not printed the mass of each box since it can easily be read off from the given data. Conveniently for each $(\lambda_1, \lambda_\infty)$ there is at most one $c \in \mathcal{C}(411, \lambda_1, \lambda_\infty)$ with $|\mathrm{Aut}(X)| > 1$. The corresponding $\mathrm{Gal}(X)$, if it exists, is printed after a decimal point. The fractional values appearing are

$$\begin{aligned} S_4, S_4^t, S_{42}, S_{42}^t &\longmapsto .5 \\ D_4, D_4^t &\longmapsto .25 \\ C_4, C_{42} &\longmapsto .125, \end{aligned}$$

as follows from the tables in Section 4.

Genera. The possibilities for the degree sets $\{n_i\}$ are $\{4,1,1\}, \{4,2\}$,

$\{5,1\},\{6\}$. If $n_j \in \{1,2\}$, then $g_j = 0$. If $n_j \in \{4,5,6\}$, then $g_j \in \{0,1\}$. A group is printed in boldface if and only if the corresponding large degree component has $g_j = 1$.

Twinning. The existence of the sextic twinning operator forces the evident symmetry of the table, emphasized by our drawing of horizontal and vertical lines. For example, $\mathcal{C}(411, 3111, 321)$ is represented by two covers $\overline{X}_1$ and $\overline{X}_2$, both with Galois group S_5; each of these is a disjoint union of two genus 0 curves. Necessarily the $\mathcal{C}(411, 33, 6)$ is represented by the twin curves $\overline{X}_1^t$ and $\overline{X}_2^t$ with Galois group $S_5^t = PGL_2(\mathbf{F}_5)$; each of these is a single genus 1 curve.

Rigidity. When a mass 1 group appears just once in a given box the corresponding cover is rigid. This implies that the cover of $\mathbf{P}^1_{\mathbf{C}}$ is the base-change of a cover of $\mathbf{P}^1_{\mathbf{Q}}$. For example, in general one has $|\mathcal{C}(n-1, 2, n)| = 1$, the cover being given by the remarkably simple equation $x^n - ntx + (n-1)t = 0$ with Galois group S_n. This general fact is illustrated by our boxes (3111,21111) and (51,21111) for $n = 4$ and $n = 5$, respectively. All the remaining cases where no elliptic curves are present are mentioned in [**8**]; remarkable number fields appear as fields of moduli.

One reason we have presented the above table is for comparison with the results of [**11**] and [**7**]. A central role in [**11**] is played by a p-adic mass formula, due to Serre and Krasner. This formula is similar to the above formula in that automorphism groups appear but Galois groups do not. In [**7**] playing the role of $\mathbf{P}^1$ is a "compactified version" of Spec $(\mathbf{Z})$. Playing the role of $\{0, 1, \infty\}$ are the three "primes" $\{\infty, 2, 3\}$. In this number-theoretic setting there is no known mass formula; the complete list of sextic algebras is found by an exhaustive computer search.

REFERENCES

1. G. Butler and J. McKay, *The transitive groups of degree up to* 11, Comm. in Alge. **11** (1983), 863–911.

2. J.H. Conway, et al., *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

3. K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), 289–307.

4. ———, *On invariant polynomials and their application in field theory*, Math. Comp. **48** (1987), 781–797.

5. ———, *Specht modules and resolvents of algebraic equations*, J. Algebra **137** (1991), 12–43.

6. A. Grothendieck et al., *Revêtements étales et groupe fondamental* (1961), Lecture Notes in Math. **224** (1971).

7. J. Jones and D. Roberts, *Sextic number fields with discriminant* $-^j 2^a 3^b$, to appear in the Proc. of the Fifth Conf. of the Canadian Number Theory Association.

8. G. Malle, *Fields of definition of some three point ramified fields extensions*, in *The Grothendieck theory of dessins d'enfants* (Leila Schneps, ed.), Cambridge University Press, New York, 1994.

9. G.A. Miller, *The collected works of George Abram Miller*, Volumes I–IV, University of Illinois Press, Urbana, 1936–1955.

10. J. Milne, *Étale cohomology*, Princeton University Press, Ewing, 1980.

11. D. Roberts, *Tables of p-adic fields*, in preparation.

12. J.-P. Serre and H. Darmon, *Topics in Galois theory*, Jones and Bartlett Publishers, Boston, 1992.

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Current address: Department of Mathematics, Rutgers University, Piscataway, New Jersey 08854-8019
E-mail address: davrobts@math.rutgers.edu