J. Korean Math. Soc. **44** (2007), No. 1, pp. 199–210

GALOIS THEORY OF MATHIEU GROUPS IN CHARACTERISTIC TWO

Ikkwon Yie

Abstract. Given a field K and a finite group G, it is a very interesting problem, although very difficult, to find all Galois extensions over K whose Galois group is isomorphic to G. In this paper, we prepare a theoretical background to study this type of problem when G is the Mathieu group M_{24} and K is a field of characteristic two.

1. Introduction

Let k be a field of characteristic $p > 0$. Every Galois extension of k with cyclic Galois group of order p is obtained as the splitting field of the Artin-Schreier polynomial $Y^p - Y + a$ for some $a \in k$. In [7] Saltman generalized this idea and developed the theory of generic extensions. It is said that there is a generic extension for a finite group G over a field K if there is a ring extension of finite K-algebras such that every Galois extension of K with Galois group G can be obtained as a specialization of this ring extension. Abelian groups are basic concrete examples to this theory arising from the theory of Kummer extensions and the Artin-Schreier polynomial. Saltman also proves that semidirect products and wreath products of groups have generic extensions under certain conditions.

However, if it comes to a specific group, it is very difficult to decide whether there is a generic extension. To lay a theoretical background to investigate this problem for the largest Mathieu group M_{24} in characteristic two is our purpose in this paper. Note that concrete polynomials are written down in [2, 4, 5, 8] and are shown to have Mathieu groups as their Galois groups using what Abhyankar called linearization process. We start with a new look on these applications of linearization process from group representation point of view.

It is generally understood that the outcome of the linearization process provides a modular representation of the Galois group in the splitting field of given polynomial. In fact, this is not a peculiar phenomenon that occurs only when

Received November 19, 2005.

2000 *Mathematics Subject Classification.* Primary 13B05; Secondary 20C05, 12E20.

Key words and phrases. Mathieu groups, generic extension, linearization.

This work was done while the author was visiting Purdue University. The author is grateful for the hospitality and support received from the Math Department.

one can apply the linearization process. Rather, 'essentially' every representation of a finite group G can be found in Galois extensions with Galois group G. More precisely, we will prove, in section 2, the following theorem and then present as examples the cases when G is one of the Mathieu groups and the representations are binary Golay codes and Todd modules.

Theorem 1.1. *Let L be a finite Galois extension over a field K with the Galois group G.*

(1) *If we fix a normal basis $\mathcal{N}$ for L, then L becomes a left module over the group algebra $K[G]$, which is isomorphic to $K[G]$. Thus for every left ideal I of $K[G]$, there is a K-subspace V of L which is a $K[G]$-submodule isomorphic to I.*
(2) *Fix a normal basis $\mathcal{N}$ and regard L as $K[G]$ as above. Let $J \subset I$ be left ideals of $L(=K[G])$. Suppose I, J are defined over a finite subfield k of K. That is, suppose I, J have (K-)generating sets which belong to the k-span of $\mathcal{N}$. Then there is a K-subspace W of L which is a $K[G]$-submodule isomorphic to I/J.*

Note that Abhyankar implicitly proves this theorem for faithful representations in section 3 of [3]. That is, given any faithful representation V of G over k, he finds a k-subspace of L which is isomorphic to the representation on the dual space V' of V. Since the isomorphism between dual vector spaces is not natural, the subspace Abhyankar found may not be isomorphic to V as representations unless some special conditions are satisfied (e.g., G is contained in the orthogonal group $O(V)$). Our proof deals directly with the representation and submodules of L. Also note that the subrepresentation W of L in the theorem doesn't have to be faithful. If the kernel of the representation W is $H \lhd G$, then $K(W)$ is a Galois extension with Galois group G/H.

In section 3, we will prove as direct consequences of the observations made in the examples in section 2 that EVERY Mathieu group (of degree 12, 23, or 24) extensions can be found using the linearization technique. We also provide the linearization process written as an algorithm that can be readily coded into a computer program.

In section 4, we make observations on the Galois theoretic relations of M_{23} as a point stabilizer inside M_{24}. The construction of extended binary Golay code $\mathcal{G}_{24}$ from the Golay code $\mathcal{G}_{23}$ will be vividly realized in the Galois theoretical context. Moreover, it is a remarkable fact that all known polynomials $\overline{F}$ in characteristic two with Galois group M_{24} are of the form $\overline{F} = YF + T$, where F is a polynomial of degree 23 with Galois group M_{23} and T is an indeterminate. We will show that this is an aspect of a general phenomena. Namely, we will prove:

Theorem 1.2. *Let K be a field of characteristic two and $F = F(Y)$ be a monic polynomial of degree 23 over K whose Galois group is M_{23}. If we let*

$\overline{F} = \overline{F}(Y) = YF(Y) + T \in K(T)$, *where T is an indeterminate over K, then the Galois group of $\overline{F}$ over $K(T)$ is M_{24}.*

In section 5, by analyzing the Todd modules generated by the roots, we will prove that a few coefficients of certain degree terms of Mathieu group polynomials should vanish. By speculating the steps of linearization process and the correspondence of M_{24} polynomials with M_{23} polynomials we claim that more coefficients should vanish.

The author would like to express his gratitude to Professor Abhyankar for inspiring conversations and encouragement in preparing this paper.

2. Group representations in Galois extensions

In this section, we prove Theorem 1.1. The part (1) is obvious and self explanatory. To prove part (2), we need Proposition (2.2) in [3], which is the vectorial part of the following lemma. Let us first prepare the terminology.

Let p be a prime and q be a positive power of p. Let k be the field of q elements and K be a field containing k. By a vectorial (resp., affine) q-polynomial (over K) of q-degree m, we mean a polynomial of the form $\Lambda = \sum_{i=0}^{m} a_i Y^{q^{m-i}}$ (resp., $\Lambda' = \sum_{i=0}^{m} a_i Y^{q^{m-i}} + a_\infty$), where $a_0, a_1, \ldots, a_m, a_\infty \in K$ and $a_0 \neq 0$. When L is an overfield of K, it is clear that the set W of roots in L of a vectorial q-polynomial Λ over K form a vector space over k and the set W' of roots in L of the affine q-polynomial $\Lambda + C$ with $C \in K$ is an 'affine translate' of W. The converse of this is also true:

Lemma 2.1. *Let K be a field containing a subfield k of q elements. Let W be an m dimensional vector subspace of K over k. Then*

(1) *$\Lambda = \prod_{w \in W}(Y - w)$ is a vectorial q-polynomial over K of q-degree m;*

(2) *$\Lambda' = \prod_{w \in W}(Y - w - c)$ with $c \in K$ is an affine q-polynomial over K of q-degree m.*

Proof. The affine part follows immediately from the vectorial part by noting $\Lambda'(Y) = \Lambda(Y-c) = \Lambda(Y) - \Lambda(c)$. The vectorial part can be proved by induction. If $m = 1$, then $W = \{\alpha b \mid \alpha \in k\}$ for some $b \in W$ and

$$\Lambda(bY) = \prod_{\alpha \in k}(bY - \alpha b) = b\prod_{\alpha \in k}(Y - \alpha) = b^q(Y^q - Y) = (bY)^q - b^{q-1}(bY).$$

Thus $\Lambda(Y) = Y^q - b^{q-1}Y$. Now suppose $\Lambda(Y) = \prod_{w \in W}(Y - w)$ is a vectorial q-polynomial and $\overline{W}$ is the k-span of $W \cup \{\bar{b}\}$ for some element $\bar{b} \in K$. Then

$$\begin{aligned}\overline{\Lambda}(Y) &= \prod_{\bar{w} \in \overline{W}}(Y - \bar{w}) = \prod_{\alpha \in k}\left(\prod_{w \in W}(Y - \alpha\bar{b} - w)\right) \\ &= \prod_{\alpha \in k}\Lambda(Y - \alpha\bar{b}) = \prod_{\alpha \in k}(\Lambda(Y) - \alpha\Lambda(\bar{b})) \\ &= (\Lambda(Y))^q - (\Lambda(\bar{b}))^{q-1}\Lambda(Y)\end{aligned}$$

is a vectorial q-polynomial. □

Now we come back to the proof of Theorem 1.1. Since I (resp., J) is a $K[G]$-submodule defined over k, there is a finite subset B_I (resp., B_J) of $\operatorname{span}_k(\mathcal{N})$, the k-span of $\mathcal{N}$, which is mapped onto itself by G and spans I (resp., J) as a K-vector space. Let $\mathcal{C} = \operatorname{span}_k(B_J)$. Then by Lemma 2.1,

$$\Phi(Y) = \prod_{v \in \mathcal{C}} (Y - v)$$

is a vectorial q-polynomial, where q is the number of elements in k. We have $\Phi(Y) \in K[Y]$ because $\mathcal{C}$ is mapped onto itself by G. Define a K-linear map $\phi : I \to L$ by setting $\phi(w) = \Phi(w)$, for each $w \in B_I$. Clearly, ϕ is a $K[G]$-module homomorphism whose kernel is J. It follows that the image $\phi(I) \in L$ is isomorphic to I/J as $K[G]$-module.

Before closing this section, we present examples which will be the main objects of study in this paper. In these examples, we let K be a field of characteristic two and k be its prime subfield and we deal only with $k[G]$-modules rather than $K[G]$-modules. Let L be a Galois extension of K with Galois group G and suppose we have fixed a normal basis $\mathcal{N} = \{\sigma(\beta) \mid \sigma \in G\}$.

Example 1. Take $G = M_{23}$, the Mathieu group of degree 23. Let H be a subgroup of G of index 23 and $H_1 = H, H_2, \ldots, H_{23}$ be the left cosets of H. Let $\bar{b}_i = \sum_{\sigma \in H_i} \sigma(\beta)$ for $i = 1, \ldots, 23$. Then $\overline{B} = \{\bar{b}_i \mid i = 1, \ldots, 23\}$ is linearly independent over K and mapped onto itself by G and $\overline{V} = \operatorname{span}_k(\overline{B})$ is the usual permutation module of G. There is a 12-dimensional subspace in $\overline{V}$ which is mapped onto itself by G, i.e., the Golay code $\mathcal{G}_{23}$. Then the quotient of $\overline{V}$ by $\mathcal{G}_{23}$ is the Todd module for G (the cocode of $\mathcal{G}_{23}$) and has an isomorphic copy $V = \Phi(\overline{V})$ in L of k-dimension 11, where Φ is the vectorial 2-polynomial having $\mathcal{G}_{23}$ as the set of roots and regarded as a function on $\overline{V}$. Note that V is partitioned into 4 subsets in terms of the weight of the vectors. Namely, the set $B_0 = \{0\}$ consisting only of 0 vector (weight 0), the set $B_1 = \Phi(\overline{B})$ of $\binom{23}{1} = 23$ vectors of weight 1, the set B_2 of $\binom{23}{2} = 253$ vectors of weight 2, and the set B_3 of $\binom{23}{3} = 1771$ vectors of weight 3. Also note that G acts faithfully and transitively on each B_i for $i = 1, 2, 3$ and hence $K(B_1) = K(B_2) = K(B_3) = L$. The action of G on B_1 is the usual 4-transitive permutation action of M_{23} of degree 23.

Example 2. Take $G = M_{24}$, the Mathieu group of degree 24. Let H be a subgroup of G of index 24 and $H_0 = H, H_1, \ldots, H_{23}$ be the left cosets of H. Let $\bar{b}_i = \sum_{\sigma \in H_i} \sigma(\beta)$ for $i = 0, \ldots, 23$. Then $\overline{B} = \{\bar{b}_i \mid i = 0, \ldots, 23\}$ is linearly independent over K and mapped onto itself by G and $\overline{V} = \operatorname{span}_k(\overline{B})$ is the usual permutation module of G. There is a 12-dimensional subspace in $\overline{V}$ which is mapped onto itself by G, i.e., the extended Golay code $\mathcal{G}_{24}$. Then the quotient of $\overline{V}$ by $\mathcal{G}_{24}$ is the 12-dimensional Todd module for G (the cocode of $\mathcal{G}_{24}$) and has an isomorphic copy $V = \Phi(\overline{V})$ in L where Φ is the vectorial 2-polynomial having $\mathcal{G}_{24}$ as the set of roots and regarded as a function on $\overline{V}$. Note that V is partitioned into 5 subsets in terms of the weight of the vectors. Namely, the set $B_0 = \{0\}$ consisting only of 0 vector (weight 0), the set $B_1 = \Phi(\overline{B})$ of $\binom{24}{1} = 24$ vectors of weight 1, the set B_2 of $\binom{24}{2} = 276$ vectors of weight 2, the set B_3 of $\binom{24}{3} = 2024$ vectors of weight 3, and the set B_4 of $\binom{24}{4}/6 = 1771$ vectors of weight 4. Again G acts faithfully and transitively on each B_i for $i = 1,2,3,4$ and hence $K(B_1) = K(B_2) = K(B_3) = K(B_4) = L$. The action of G on B_1 is the usual 5-transitive permutation action of M_{24} of degree 24. Also note that $V_0 = B_0 \cup B_2 \cup B_4$ is the 11-dimensional Todd module for G and $V_1 = B_1 \cup B_3$ becomes an affine translate of V_0.

Example 3. Take $G = M_{12}$, the Mathieu group of degree 12. Let H be a subgroup of G of index 12 and $H_1 = H, H_2, \ldots, H_{12}$ be the left cosets of H. Let $\bar{b}_i = \sum_{\sigma \in H_i} \sigma(\beta)$ for $i = 1, \ldots, 12$. Then $\overline{B} = \{\bar{b}_i \mid i = 1, \ldots, 12\}$ is linearly independent over K and mapped onto itself by G and $V = \mathrm{span}_k(\overline{B})$ is the usual permutation module of G. It is a well known fact that G has other subgroup H' of index 12 which is abstractly isomorphic to H but not conjugate to H in G. Let $H_1' = H', H_2', \ldots, H_{12}'$ be the left cosets of H' and let $\bar{b}_i' = \sum_{\sigma \in H_i'} \sigma(\beta)$ for $i = 1, \ldots, 12$. Then $\overline{B}' = \{\bar{b}_i' \mid i = 1, \ldots, 12\}$ is linearly independent over K and mapped onto itself by G and $V' = \mathrm{span}_k(\overline{B}')$ is the usual permutation module of G but not equivalent to V.

Note that M_{12} is a subgroup of M_{24} and the restriction of the usual permutation module $\overline{V}$ of M_{24} to the subgroup $G = M_{12}$ is isomorphic to $V \oplus V'$. However, the $k[G]$-submodule $V + V'$ of L is of one less dimension (over k) due to the fact that $\sum_{i=1}^{12} \bar{b}_i = \sum_{i=1}^{12} \bar{b}_i' = \sum_{\gamma \in \mathcal{N}} \gamma$. Denote this common value by α. If we let $\mathcal{G}$ to be the image of the Golay code submodule $\mathcal{G}_{24}$ of $V \oplus V'$ under the obvious map of $V \oplus V'$ onto $V + V'$, then $\alpha \in \mathcal{G}$. Therefore the quotient module $(V + V')/\mathcal{G}$ is isomorphic to the cocode of $\mathcal{G}_{24}$ (the Todd module of M_{24} restricted to G) and has an isomorphic copy $W = \Phi(V + V')$ in L of k-dimension 12, where Φ is the vectorial 2-polynomial having $\mathcal{G}$ as the set of roots and regarded as a function on $V + V'$.

Just like the case of M_{24}, the set W_0 of vectors in W of even weight becomes a $k[G]$-submodule of k-dimension 11 and the set W_1 of vectors in W of odd weight becomes an affine translate of W_0. The 24 vectors of weight 1 are grouped into two sets of 12 vectors, that is, $B = \Phi(\overline{B})$ and $B' = \Phi(\overline{B}')$ on each of which G acts faithfully and 5-transitively. It follows that $K(B) = K(B') = L$. The one point stabilizer H (of the G-action on B) acts 3-transitively on B' and the one point stabilizer H' (of the G-action on B') acts 3-transitively on B.

What is different from the case of M_{24} is that W has two nonequivalent submodules $\widetilde{V} = \Phi(V) = \mathrm{span}_k(B)$ and $\widetilde{V}' = \Phi(V') = \mathrm{span}_k(B')$ of k-dimension 11. The three distinct 11-dimensional submodules $W_0, \widetilde{V}, \widetilde{V}'$ intersect in a 10-dimensional submodule $\widetilde{W_0}$, which is a simple $k[G]$-module. Then, $\widetilde{W_1} = \widetilde{V} \backslash \widetilde{W_0}$

(resp., $\widetilde{W_1'} = \widetilde{V}' \setminus \widetilde{W_0}$) is an affine translate of $\widetilde{W_0}$ which contain B (resp., B'). Note that we have $W_0 \cup \widetilde{V} \cup \widetilde{V}' = W$ and $\widetilde{W_1} \cup \widetilde{W_1'} = W_1$.

Remark 1. We can make up a similar situation as the last paragraph of Example 3 as following. Let t be any element in K but not in $\widetilde{V}$ and let $b_i^* = b_i + t$ for $i = 1, \ldots, 12$. Then $\widetilde{V}^* = \mathrm{span}_k(B^*)$, where $B^* = \{b_1^*, \ldots, b_{12}^*\}$, is a $k[G]$-module isomorphic to $\widetilde{V}$ and intersects with $\widetilde{V}$ in W_0. Therefore $W^* = \widetilde{V} + \widetilde{V}^*$ is a $k[G]$-module of degree 12 which is not isomorphic to W. In Theorem 4.2 of [8], W^* was constructed from a pair of degree 12 polynomials and shown to be isomorphic to the cocode (the ambient space modulo the code) of the doubly even binary code of length 24 and minimal weight 4.

However, this code is not very useful in computing Galois group because the group of automorphisms of this code contains an isomorphic copy of S_{12}.

Example 4. Take $G = \mathrm{Aut}(M_{12})$, the group of automorphisms of M_{12}. Then the two isomorphic subgroups H and H' of M_{12} of index 12 which are not conjugates in M_{12} become conjugates in G. Let $H_1 = H, H_2, \ldots, H_{24}$ be the left cosets of H. Let $\bar{b}_i = \sum_{\sigma \in H_i} \sigma(\beta)$ for $i = 1, \ldots, 24$. Then $\overline{B} = \{\bar{b}_i \mid i = 1, \ldots, 24\}$ is linearly independent over K and mapped onto itself by G and $V = \mathrm{span}_k(\overline{B})$ is a $k[G]$-module of k-dimension 24. Note that $G = \mathrm{Aut}(M_{12})$ is a subgroup of M_{24} and the restriction of the usual permutation module $\overline{V}$ of M_{24} to the subgroup G is isomorphic to V. Therefore the quotient module $V/\mathcal{G}_{24}$ is isomorphic to the cocode of $\mathcal{G}_{24}$ and has an isomorphic copy $W = \Phi(V)$ in L of k-dimension 12, where Φ is the vectorial 2-polynomial having $\mathcal{G}_{24}$ as the set of roots and regarded as a function on $\overline{V}$. Just like the case of M_{24}, the set W_0 of vectors in W of even weight becomes a $k[G]$-submodule of k-dimension 11 and the set W_1 of vectors in W of odd weight becomes an affine translate of W_0.

3. Linearization

In [2], Abhyankar determined the Galois group of $Y^{23} + XY^3 + 1$ over $k(X)$, where k is a field of characteristic two, to be the Mathieu group M_{23} using the technique which he called linearization. In [4], Abhyankar and Yie determined the Galois group of the similar looking polynomial $Y^{24} + XY^4 + Y + T$ over $k(X, T)$ to be the Mathieu group M_{24} using practically the same computation of linearization process as above. Again using the linearization process in [5], Abhyankar and Yie found polynomials whose Galois groups are the small Mathieu groups M_{12} and M_{11}. In [8], Yie found the polynomial $Y^{24} + UY^{16} + (U^4 + V^6)Y^8 + XY^4 + UVY^2 + Y + T$, which embraces all the above mentioned polynomials as various specializations of it, then determined the Galois group over $k(U, V, X, T)$ to be the Mathieu group M_{24}.

Due to the highly transitive nature of Mathieu groups, it was hard to tell them apart from the alternating or symmetric groups in computing Galois groups, and so far this linearization process is the only successful method. The following theorems tell us that every Mathieu group extensions can be found using linearization technique.

Theorem 3.1. *Let K be a field of characteristic two and L be a Galois extension over K with Galois group M_{23}. Then L is the common splitting field of irreducible polynomials F_1 of degree 23, F_2 of degree 253, and F_3 of degree 1771 in $K[Y]$ such that $\Lambda = YF_1F_2F_3$ is a vectorial 2-polynomial over K of 2-degree 11.*

Proof. Let V be the Todd module constructed in Example 1 of the previous section and B_0, B_1, B_2, B_3 be the partition of V in terms of weight. Then $F_i = \prod_{r\in B_i}(Y-r)$ for $i = 1, 2, 3$ are irreducible over K since the Galois group acts transitively on each B_i's. It follows that $\Lambda = YF_1F_2F_3 \in L[Y]$ is a vectorial 2-polynomial of 2-degree 11 since the vector space $V = \cup_{i=0}^{3}B_i$ of dimension 11 over GF(2) is the set of roots of Λ in L. □

Theorem 3.2. *Let K be a field of characteristic two and L be a Galois extension over K with Galois group M_{24}. Then L is the common splitting field of irreducible polynomials F_1 of degree 24, F_2 of degree 276, F_3 of degree 2024, and F_4 of degree 1771 in $K[Y]$ such that $\Lambda_1 = F_1F_3$ is an affine 2-polynomial over K of 2-degree 11, $\Lambda_0 = YF_2F_4$ is a vectorial 2-polynomial over K of 2-degree 11 which differs from Λ_1 by a constant in K, $\Lambda = \Lambda_0\Lambda_1$ is a vectorial 2-polynomial over K of 2-degree 12.*

Proof. Let V be the Todd module constructed in Example 2 of the previous section and B_0, B_1, B_2, B_3, B_4 be the partition of V in terms of weight. Then $F_i = \prod_{r\in B_i}(Y-r)$ for $i = 1, 2, 3, 4$ are irreducible over K since the Galois group acts transitively on each B_i's. It follows that $\Lambda = YF_1F_2F_3F_4 \in K[Y]$ is a vectorial 2-polynomial of 2-degree 12 since the vector space $V = \cup_{i=0}^{3}B_i$ over GF(2) is the set of roots in L. Also, the two factors $\Lambda_0 = YF_2F_4$ and $\Lambda_1 = F_1F_3$ in $K[Y]$ are respectively a vectorial 2-polynomial and an affine 2-polynomial of 2-degree 11 which differ by a constant in K since the subspace $V_0 = B_0 \cup B_2 \cup B_4$ and its affine translate $V_1 = B_1 \cup B_3$ are their respective sets of roots in L. □

Theorem 3.3. *Let K be a field of characteristic two and L be a Galois extension over K with Galois group M_{12}. Then L is the common splitting field of two irreducible polynomials F and F' of degree 12 over K and two affine 2-polynomials Ψ and Ψ' of 2-degree 10 over K such that*

(1) *Ψ (resp., Ψ') is a multiple of F (resp., F');*
(2) *Ψ and Ψ' are differ by a constant in K.*

It follows that $\Lambda_1 = \Psi\Psi'$ is an affine 2-polynomial over K of 2-degree 11 which is a multiple of FF'. Moreover, if $b \in L$ (resp., $b' \in L$) is a root of F (resp., F') then F' (resp., F) remains irreducible over $K(b)$ (resp., $K(b')$).

Proof. We use the various subsets of the Todd module W constructed in Example 3 of the previous section. Let $F = \prod_{r\in B}(Y-r)$, $F' = \prod_{r'\in B'}(Y-r')$,

$\Psi = \prod_{r\in\widetilde{W}_1}(Y-r)$, and $\Psi' = \prod_{r\in\widetilde{W}_1'}(Y-r)$. The two polynomials F, F' of degree 12 are irreducible over K because the Galois group acts transitively on each of B and B'. The generating set B (resp., B') of $\widetilde{V}$ (resp., $\widetilde{V}'$) is contained in the affine translate $\widetilde{W}_1$ (resp., $\widetilde{W}_1'$) of the subspace $\widetilde{W}_0$. Therefore, the two polynomials Ψ, Ψ' are affine 2-polynomials of 2-degree 10 over K which differ by a constant. Obviously, Ψ (resp., Ψ') is a multiple of F (resp., F'). It follows that L is the common splitting field of F and F', hence also of Ψ and Ψ' since the action of the Galois group on each of B and B' is faithful.

For $b_0 \in B$ (resp., $b_0' \in B'$), we have $\mathrm{Gal}(L, K(b_0)) = H$ (resp., $\mathrm{Gal}(L, K(b_0'))$ $= H'$). However, the action of H (resp., H') on the set B' (resp., B) of roots of F' (resp., F) are 3-transitive. Thus F' (resp., F) is irreducible over $K(b)$ (resp., $K(b')$). □

Note that the polynomials mentioned at the beginning of this section are related with Todd modules like the polynomials in above theorems. The reason why polynomials related with permutation modules are not used in constructing Mathieu group extensions is because the vectorial 2-polynomials which are multiples of such polynomials must have 2-degree at least one less the degree and it is very hard to extract information about the Galois groups.

In order to describe generic extensions, if any, for Mathieu groups in concrete form, it is inevitable to apply the linearization process to polynomials with indeterminate coefficients and this process can be fairly complicated as is shown in Appendix of [8]. For future reference, we briefly describe the process of finding the vectorial polynomial which is a multiple of given polynomial.

Linearization Algorithm

Input: A polynomial $F \in K[Y]$ of degree n, where K is a field of characteristic $p > 0$

Output: An affine p-polynomial of p-degree N which is a multiple of F for an appropriate $N \leq n$

Synopsis: $\Lambda[j]$ is an affine p-polynomial of p-degree j which is congruent to $F[j]$ of degree $< n$ modulo F. We say that F is linearized at N.

```
(1) Set $\Lambda[m-1] = F[m-1] = Y^{p^{m-1}}$, where $p^{m-1} < n \leq p^m$.
(2) For $m \leq j \leq N$ repeat:
    (a) Set $\Lambda'[j] = \Lambda[j-1]^p$ and $F'[j] =$ the reduction of $F[j-1]^p$ modulo $F$.
    (b) Collect the terms of $F'[j]$ of $Y$-degree 0 and power of $p$ to form an affine $p$-polynomial $\Delta$ and set $F[j] = F'[j] - \Delta$ and $\Lambda[j] = \Lambda'[j] - \Delta$.
(3) Find $A_j \in K[Y]$ for $j = m, \ldots, N$ such that $\sum_{j=m}^{N} A_j F[j] = 0$.
(4) Output $\Lambda = \sum_{j=m}^{N} A_j \Lambda[j]$.
```

Remark 2. Let D be an integrally closed subdomain of K and suppose $F \in D[Y]$. (In most of practical applications, D is a polynomial ring over a finite field k in several variables and K is the quotient field of D.) Then $\Lambda \in D[Y]$.

4. Interactions of Mathieu groups of degrees 23 and 24

This section is divided into two parts. The first part deals with downward interaction - from M_{24} to its point stabilizer M_{23}. Here, we study Galois correspondence of M_{23} as a point stabilizer of M_{24} inside a Galois extension with Galois group M_{24}. The second part deals with upward interaction - from M_{23} to its transitive extension M_{24}. Here, we prove Theorem 1.2.

From M_{24} to M_{23}: Let us denote the Mathieu group M_{24} by G and a subgroups of index 24 by H. Then H is isomorphic to the Mathieu group M_{23}. We want to study the Galois theoretic counterpart of this subgroup $H < G$ with respect to the Todd modules as appeared in section 2 and the defining equations of the Galois extension as appeared in section 3.

Suppose, for the time being, we are in the situation of Example 2 and let symbols represent the same objects. Thus, K is a field of characteristic two, k is its prime subfield and L is a Galois extension with Galois group $G = M_{24}$. The usual permutation $k[G]$-module $\overline{V}$ is realized in L as $\mathrm{span}_k(\overline{B})$, where $\overline{B} = \{\bar{b}_i \mid i = 0, \dots, 23\}$ is a K-linearly independent subset L on which G has 5-transitive action. The subgroup H is the point stabilizer of $\bar{b}_0$ of this action.

Then H is the Galois group of L over its fixed field $K_0 = K(\bar{b}_0)$. Let $\bar{c}_i = \bar{b}_i - \bar{b}_0$ for $i = 1, \dots, 23$. It follows that $\overline{C} = \{\bar{c}_i \mid i = 1, \dots, 23\}$ is linearly independent over K_0 and $\overline{W} = \mathrm{span}_k(\overline{C})$ becomes the usual permutation module of H (with respect to the basis $\overline{C}$). The extended Golay code $k[G]$-submodule $\mathcal{G} = \mathcal{G}_{24}$ of $\overline{V}$ is contained in $\overline{W}$ as a subset and becomes the Golay code $k[H]$-submodule $\mathcal{G}_{23}$ of $\overline{W}$ (with respect to the basis $\overline{C}$). Note that this situation perfectly fits into the construction of the extended code $\mathcal{G}_{24}$ from $\mathcal{G}_{23}$ using $\bar{b}_0$ as the parity check bit.

The vectorial 2-polynomial Φ having $\mathcal{G}$ as the set of roots can be thought of as a $k[G]$-module homomorphism of $\overline{V}$ into L and does map $\overline{V}$ onto the 12-dimensional Todd module V for G. We have a partition $V = B_0 \cup B_1 \cup B_2 \cup B_3 \cup B_4$ of V in terms of weight. The subset $V_0 = B_0 \cup B_2 \cup B_4$ consisting of vectors of even weight is the 11-dimensional Todd module for G.

Note that Φ can also be thought of as a $k[H]$-module homomorphism of $\overline{W}$ into L. By the definition, each vector of $\overline{W}$ is mapped by Φ onto a vector of even weight (as a vector in V). Thus the Todd module $W = \Phi(\overline{W})$ for H coincides with V_0 as a set.

Now, we also make use of the notations of Theorem 3.2 and its proof. Thus $F_i = \prod_{r \in B_i}(Y - r)$ for $i = 1, 2, 3, 4$ are irreducible over K and $\Lambda_0 = YF_2F_4$ and $\Lambda_1 = F_1F_3$ in $K[Y]$ are respectively a vectorial 2-polynomial and an affine 2-polynomial of 2-degree 11 which differ by a constant in K. Let $b_i = \Phi(\bar{b}_i)$ for $i = 0, 1, \dots, 23$. Then the action of G on $B_1 = \Phi(\overline{B}) = \{b_0, b_1, \dots, b_{23}\}$ is equivalent to that of G on $\overline{B}$. It follows that the 'root field' of F_1 is $K(b_0) = K(\bar{b}_0) = K_0$.

Let $c_i = b_i - b_0$ for $i = 1, \dots, 23$. Then the action of H on $C = \Phi(\overline{C}) = \{c_1, \dots, c_{23}\}$ is equivalent to that of H on $\overline{C}$. Note that $F_1' = \prod_{i=1}^{23}(Y - c_i) = \frac{1}{Y}[F_1(Y + b_0) - F_1(b_0)]$ is what Abhyankar calls 'the twisted derivative' of F_1. It follows from 5-transitivity of G that F_1' is irreducible over K_0. The Todd module W for H is spanned by the set C of roots of F_1'. Note that W is the set of roots of Λ_0. Therefore, over K_0, F_4 remains irreducible while F_2 factors into F_1' and an irreducible factor of degree 253.

From M_{23} to M_{24}: We now turn to the proof of Theorem 1.2. Thus, let K be a field of characteristic two and $F = F(Y)$ be a monic polynomial of degree 23 over K whose Galois group is M_{23}. Also, let $\overline{F} = \overline{F}(Y) = YF(Y) + T \in K(T)$, where T is an indeterminate over K. We need to prove that the Galois group of $\overline{F}$ over $K(T)$ is M_{24}.

Let L be the splitting field of F over K and $\overline{L}$ be the splitting field of $\overline{F}$ over $K(T)$. Let R be the local ring $K[T]_{(T)}$ and $(S, \mathfrak{m})$ be the local ring obtained by localizing the integral closure of R in $\overline{L}$ at a maximal ideal. Note that all 24 roots of $\overline{F}$ belong to S. Let $\gamma : S \to L$ be a homomorphism obtained by extending the canonical epimorphism $R \to K$. Then the kernel of γ is $\mathfrak{m}$. Since $\overline{F}$ is mapped onto YF by γ, only one root of $\overline{F}$ is mapped to 0 and hence belongs to $\mathfrak{m}$. Therefore the decomposition group H of S is a point stabilizer of $G = \mathrm{Gal}(\overline{F}, K(T))$. It follows that G is at least 5-transitive since H is mapped onto $\mathrm{Gal}(L, K) = M_{23}$ under the map induced by γ which preserves the permutation actions of automorphisms (of fields) on the roots of corresponding polynomials. Now, any subgroup of the symmetric group S_{24} is isomorphic to M_{24}.

Remark 3. All known polynomials with Galois group M_{23} or M_{24} are related with the Todd modules, i.e., the roots generate relevant Todd module. However, we don't know whether $\overline{F}$ in Theorem 1.2 is related with the Todd module, though we strongly believe so. It would be interesting either to see the proof, or to see a counterexample.

5. Mathieu group polynomials in characteristic two

Theorem 5.1. *Let K be a field of characteristic two and let $n = 23$ or 24. Consider a polynomial $F = F(Y) = Y^n + \sum_{i=1}^{n} a_i Y^{n-i} \in K[Y]$ of degree n. Suppose the Galois group $G = Gal(F, K)$ is isomorphic (as a permutation group on the set $\mathcal{R}$ of roots of F in a splitting field) to a subgroup of the Mathieu group M_n and suppose $\mathcal{R}$ generates over the prime subfield a subspace isomorphic to the Todd module for M_n. Then $a_i = 0$ for $i = 1, 2, 3$.*

Proof. Let $b_\infty, b_0, b_1, \dots, b_{22}$ be the roots of $F(Y)$ in the splitting field. We choose, for the index set, the projective line $\Omega = \{\infty, 0, \dots, 22\}$ over the Galois field $\mathbb{F} = \mathrm{GF}(23)$ because it fits best with our proof of the theorem. We regard the Golay code $\mathcal{G}_{24}$ as a collection of certain subsets of Ω as in Chapter 11 of

[6] and follow the arithmetic conventions thereof. Thus a subset J of Ω is a codeword if and only if $\sum_{r\in J} b_r = 0$.

Here, we only present the proof for the case $n = 24$. The proof for the case $n = 23$ will follow easily by noting that $\infty \in \Omega$ is the augmented bit for parity check.

Let Q' be the set of quadratic residues in $\mathbb{F}$ and N' be the set of quadratic nonresidues of $\mathbb{F}$. Also let $Q = \{0\} \cup Q'$ and $N = N' \cup \{\infty\}$. Note that then Q and N are complementary codewords of weight 12. For indexing purpose, we give order to Ω as we would for integers and the symbol ∞. And keep in mind that arithmetic with the roots b_r is in characteristic two while the arithmetic with the indices in Ω is basically modulo 23.

$\mathbf{a_1 = 0}$: First of all, we have $a_1 = \sum_{r\in\Omega} b_r = 0$ since Ω is a codeword.

$\mathbf{a_2 = 0}$: Consider the set $S_2 = \{(r, r+s) \mid r \in \mathbb{F},\ s \in N\}$ of ordered pairs of distinct elements of Ω. Suppose two such pairs $(r, r+s), (r', r'+s') \in S_2$ produce the same unordered pair $\{r, r+s\} = \{r', r'+s'\}$. Since $-1 = 22$ is a nonresidue in $\mathbb{F}$, this is possible only when $r = r'$ and $s = s'$. Hence S_2 produce exactly 23×12 distinct unordered pairs while the 24 element-set Ω has exactly so many unordered pairs of distinct elements. Therefore we have

$$a_2 = \sum_{r,s\in\Omega,\ r<s} b_r b_s = \sum_{r\in\mathbb{F}} b_r \sum_{s\in N} b_{r+s}.$$

Note that $r + N = \{r + s \mid s \in N\}$ is a codeword for all $r \in \mathbb{F}$ since N is a codeword and $\mathcal{G}_{24}$ admits the cyclic shifts on $\mathbb{F}$ as automorphisms. It follows that $\sum_{s\in N} b_{r+s} = 0$ for all $r \in \mathbb{F}$ and hence $a_2 = 0$.

$\mathbf{a_3 = 0}$: Consider the set $S_3 = \{(r, r+s, r+t) \mid r \in \mathbb{F},\ s \in N,\ t \in Q'\}$ of ordered triples of distinct elements of Ω. Suppose two such triples $(r, r+s, r+t), (r', r'+s', r'+t') \in S_3$ produce the same unordered triples $\{r, r+s, r+t\} = \{r', r'+s', r'+t'\}$. As above, $\{r, r+s\} = \{r', r'+s'\}$ if and only if $r = r'$ and $s = s'$. Thus we fall into one of the following three cases:

(1) $r = r'$, $s = s'$, and $t = t'$;
(2) $r = r' + s'$, $r + s = r' + t'$, and $r + t = r'$;
(3) $r = r' + t'$, $r + s = r'$, and $r + t = r' + s'$;

In case (2), we get $s+s' = t'$, $s = t+t'$, and $s'+t = 0$. Similarly in case (3), we get $s+s' = t$, $s' = t+t'$, and $s+t' = 0$. Out of 11×6 (unordered) pairs of distinct elements in N, 11×3 pairs add up to a quadratic residue. It is best to look at examples to study the relations of these pairs. For example, let us take the pair $5 + 7 = 12$. There are two notable aspects of these pairs. The first aspect is that for each such pairs, there are two more pairs that altogether form a family. Namely, for the example $5+7 = 12$, we have $7+11 = 18$ and $11+5 = 16$. Note that then $12+18 = 7$, $18+16 = 11$, and $16+12 = 5$. The other aspect is that for a given such pair, we have two ways to complete the complementary pairs of elements in Q'. Namely, for the example $5 + 7 = 12$, we have $5 = 16 + 12$ and $7 + 16 = 0$ in case (2), and $7 = 12 + 18$ and $5 + 18 = 0$ in case (3).

Therefore, three triples $(0, 0+5, 0+16)$, $(16, 16+7, 16+12)$, $(5, 5+11, 5+18)$ produce the same unordered triples as in case (2), and three triples $(0, 5, 12)$, $(5, 5+7, 5+18)$, $(12, 12+11, 12+16)$ produce the same unordered triples as in case (3). Hence S_3 will produce $23 \times 12 \times 11 - 23 \times 2 \times 2 \times 11 = 23 \times 11 \times 8$ distinct unordered triples out of which $23 \times 11 \times 2$ triples are repeated three times. Note that the 24 element-set Ω has $23 \times 11 \times 8$ unordered triples of distinct elements. Therefore we have

$$a_3 = \sum_{r,s,t \in \Omega,\ r<s<t} b_r b_s b_t = \sum_{r \in \mathbb{F},\ t \in Q'} b_r b_{r+t} \sum_{s \in N} b_{r+s} = 0.$$

□

References

[1] S. Abhyankar, *Ramification theoretic methods in algebraic geometry*, Princeton University Press, 1959.

[2] ______, *Mathieu group coverings in characteristic two*, C. R. Acad. Sci. Paris Ser. I Math. **316** (1993), no. 3, 267–271.

[3] ______, *Galois embeddings for linear groups*, Trans. Amer. Math. Soc. **352** (2000), no. 8, 3881–3912.

[4] S. Abhyankar and I. Yie, *Some more Mathieu group coverings in characteristic two*, Proc. Amer. Math. Soc. **122** (1994), no. 4, 1007–1014.

[5] ______, *Small Mathieu group coverings in characteristic two*, Proc. Amer. Math. Soc. **123** (1995), no. 5, 1319–1329.

[6] J. H. Conway and N. J. A. Sloan, *Sphere packings, lattices and groups*, Springer Verlag, New York, 1993.

[7] D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), no. 3, 250–283.

[8] I. Yie, *Mathieu group coverings and Golay codes*, J. Korean Math. Soc. **39** (2002), no. 2, 289–317.

Department of Mathematics
Inha University
Inchon 402-751, Korea
E-mail address: ikyie@math.inha.ac.kr