Arithmetic of characters of generalized symmetric groups*

D. Joyner

4-12-2002

Abstract

The result here answers the following questions in the affirmative: Can the Galois action on all abelian (Galois) fields $K/Q$ be realized explicitly via an action on characters of some finite group? Are all subfields of a cyclotomic field of the form $\mathbb{Q}(\chi)$, for some irreducible character $\chi$ of a finite group $G$? In particular, we explicitly determine the Galois action on all irreducible characters of the generalized symmetric groups. We also determine the “smallest” extension of $\mathbb{Q}$ required to realize (using matrices) a given irreducible representation of a generalized symmetric group.

1 Introduction

We show that the Galois action on all abelian (Galois) fields $K/Q$ can be realized explicitly via an action on characters of a finite group. Moreover, that all subfields of a cyclotomic field are of the form $\mathbb{Q}(\chi)$, for some irreducible character $\chi$ of a finite group $G$.

Let us note that not much better can be expected. Since $G$ is a finite group, if $g \in G$ and $\pi$ is any finite dimensional complex representation of $G$ then $\pi(g)$ is of finite order. This forces the character value $\chi(g) = \text{tr} \pi(g)$ to be a sum of roots of unity. Therefore $\mathbb{Q}(\chi)$ must be a subfield of some cyclotomic field, hence abelian.

The main result of this paper is to explicitly determine the splitting field of any irreducible character $\chi$ of a generalized symmetric group $G$. Generalized symmetric groups occur in diverse parts of mathematics - in classifying linear codes up to isometry in the Hamming metric [2] and in the mathematics of the Rubik's cube [4], to mention a few.

We shall also be able to answer the following question: What is the “smallest” extension of $\mathbb{Q}$ required to realize (using matrices) a given irreducible representation of a generalized symmetric group? This is closely related to the problem of the Schur index, which was basically solved by M. Benard [1], who showed that the splitting field is equal to the field $\mathbb{Q}(\chi)$ generated by the character values (i.e., that the Schur index equals 1; in fact he proved this for a wider class of groups that we consider here). Here we answer the question “what is this field?” by effectively computing its Galois group (see Theorem 1.1 below). Benard’s result is sufficient if you know the character table of the representation. However, if the group is large then this is, in general, not computationally feasible, in which case more explicit results are useful.

The following theorem is our main result.

**Theorem 1.1.** If $K/\mathbb{Q}$ is any abelian extension then there is a generalized symmetric group $G$ and an irreducible character $\chi$ of $G$ for which $K = \mathbb{Q}(\chi)$. Moreover the Galois action on $K$ is given by Lemma 3.1.

This will be proven in the last section. Unexplained notation and definitions shall be given below.

**Acknowledgements:** We have used MAPLE and MAGMA to obtain some of the examples in this paper. I thank W. Feit for the reference to [1], M. Isaacs and A. Turull for comments, and the anonymous referee for helpful criticisms.

## 2 Background

The character theory of generalized symmetric groups is presented, for example, in [5] and in [6], so we shall be brief. We shall use the notation of [6] below.
2.1 The generalized symmetric group

Let $C_\ell = \{0, 1, \ldots, \ell - 1\}$ denote the (additive) cyclic group of order $\ell \geq 1$ (addition is modulo $\ell$), let $S_n$ denote the symmetric group of degree $n \geq 1$, and let $G$ denote the semi-direct product $G = C_\ell^n \ltimes S_n$. We think of this as the set of pairs $(v, p)$, with $v = (v_1, \ldots, v_n)$, where each $v_i \in C_\ell$, $p \in S_n$, where $S_n$ acts on $C_\ell^n$ by $p(v) = (v_{p(1)}, v_{p(2)}, \ldots, v_{p(n)})$, and multiplication given by $(v, p) \ast (v', p') = (v + p(v'), pp')$, for $(v, p), (v', p') \in G$. A group of this form, also written $S_n \text{ wr } C_\ell$, will be called a generalized symmetric group.

For any finite group $G$, let $G^*$ denote the set of equivalence classes of irreducible representations of $G$. If $G$ is abelian then $G^*$ is a group under ordinary multiplication.

2.2 Representations of some semi-direct products

The representations of a semi-direct product of a group $H$ by an abelian group $A$, $G = A \rtimes H$ (so $A$ is normal in $G$) can be described explicitly in terms of the representations of $A$ and $H$. The purpose of this section is to recall briefly how this is done.

Let $A, H$ be subgroups of $G = A \rtimes H$, with $A \subset G$ normal and abelian \(^1\). Let $f \in R(H)$ be a class function on $H$. Extend $f$ to $G$ trivially as follows: $f^0(g) = f(g)$, for $g \in H$, and $= 0$, for $g \in G - H$. Define the function $f^G = \text{ind}_H^G(f)$ induced by $f$ to be

$$\text{ind}_H^G(f)(g) = \frac{1}{|H|} \sum_{x \in G} f^0(x^{-1}gx) = \sum_{x \in G/H} f^0(x^{-1}gx). \quad (1)$$

Since $A$ is normal in $G$, $G$ acts on the vector space of formal complex linear combinations of elements of $A^*$, $\mathbb{C}[A^*] = \text{span}\{\mu \mid \mu \in A^*\}$, by $(g\mu)(a) = \mu(g^{-1}ag)$, for all $g \in G$, $a \in A$, $\mu \in A^*$. We may restrict this action to $H$, giving us a homomorphism $H \to S_{A^*}$, where $S_{A^*}$ denotes the symmetric group of all permutations of the set $A^*$. This restricted action is an equivalence relation on $A^*$ which we refer to below as the $H$-equivalence relation. Let $|A^*|$ denote the set of equivalence classes of this equivalence relation. If $\mu, \mu'$ belong to the same equivalence class then we write in this section $\mu' \sim \mu$ (in the next section, $\sim$ will be used for a different equivalence relation). \(^1\)Think of $G$ as having the multiplication rule $(a_1, h_1)(a_2, h_2) = (a_1a_2^{h_1}, h_1h_2)$, where $a^h$ denotes conjugation.
relation). When there is no harm, we identify each element of \([A^*]\) with a character of \(A\).

For each \(\mu \in [A^*]\), let \(H_\mu = \{ h \in H \mid h\mu = \mu \}\) denote the stabilizer of \(\mu\) in \(H\). Let \(G_\mu = A \rtimes H_\mu\), for each \(\mu \in [A^*]\). There is a natural projection map \(p_\mu : G_\mu \to H_\mu\) given by \((a, h) \mapsto h\), i.e., by \(p_\mu(a, h) = a\). Extend each character \(\mu \in [A^*]\) from \(A\) to \(G_\mu\) trivially by defining \(\mu(a, h) = \mu(a)\), for all \(a \in A\) and \(h \in H_\mu\). This defines a character \(\mu \in G_\mu^*\). For each \(\rho \in H_\mu^*\), say \(\rho : H_\mu \to Aut(V)\), define \(\tilde{\rho} = \rho \circ p_\mu\). For each \(\mu \in [A^*]\) and \(\rho \in H_\mu^*\) as above, let

\[ \theta_{\mu, \rho} = \text{ind}_{G_\mu}^G (\mu \cdot \tilde{\rho}). \]  

Finally, we can completely describe all the irreducible representations of \(G\).

**Lemma 2.1.** (Proposition 25 in [6], chapter 8)

(a) For each \(\mu \in A^*\) and \(\rho \in H_\mu^*\) as above, \(\theta_{\mu, \rho}\) is an irreducible representation of \(G\).

(b) Suppose \(\mu_1, \mu_2 \in A^*\), \(\rho_1 \in H_{\mu_1}^*\), \(\rho_2 \in H_{\mu_2}^*\). If \(\theta_{\mu_1, \rho_1} \cong \theta_{\mu_2, \rho_2}\) then \(\mu_1 \sim \mu_2\) and \(\rho_1 \cong \rho_2\).

(c) If \(\pi \in G^*\) then \(\pi \cong \theta_{\mu, \rho}\), for some \(\mu \in A^*\) and \(\rho \in H_\mu^*\) as above.

### 2.3 Characters of generalized symmetric groups

Let \(G = C_t^n \rtimes S_n, A = C_t^n\). Write \(\mu \in [A^*]\) as \(\mu = (\mu_1, \ldots, \mu_n)\), where \(\mu_j \in C_t^*\). Let \(\mu_1', \ldots, \mu_t'\) denote all the distinct characters which occur “in \(\mu\)”. Let \(n_1\) denote the number of \(\mu_1'\)’s “in \(\mu\)”, \(n_2\) denote the number of \(\mu_2'\)’s “in \(\mu\)”, ..., \(n_r\) denote the number of \(\mu_r'\)’s “in \(\mu\)”. Then \(n = n_1 + \ldots + n_r\). Call this the partition associated to \(\mu\). It is well-known (and easy to prove) that

\[ (S_n)_\mu = S_{n_1} \times \ldots \times S_{n_r}. \]

The Frobenius formula for the character of an induced representation specializes to the following formula.
Lemma 2.2. Let $G = C^n_t \times S_n$, let $\chi_\rho$ denote the character of $\rho$, and let $\chi$ denote the character of $\theta_{\mu,\rho}$. Then

$$\chi(v, p) = \sum_{g \in S_n/(S_n)_{\mu}} \chi_\rho^g(g pg^{-1})\mu^g(v),$$

for all $v \in C^n_t$ and $p \in S_n$. In particular, if $p = 1$ then

$$\chi(v, 1) = (\dim \rho) \sum_{g \in S_n/(S_n)_{\mu}} \mu^g(v).$$

2.4 The Frobenius-Schur indicator

Let $G$ be any finite group. In general, there are three “types” of representations of a finite group:

Definition 2.3. Let $\rho : H \to \text{Aut}(W)$ be an $n$-dimensional irreducible representation of a finite group $H$ on a complex vector space $W$. Let $\chi$ denote the character of $\rho$.

Exactly one of the following possibilities must hold:

1. One of the values of the character $\chi$ is not real. Such representations will be called complex (or type 1 or unitary).

2. All the values of $\chi$ are real and $\rho$ is realizable by a representation over a real vector space. Such representations will be called real (or type 2 or orthogonal).

3. All the values of $\chi$ are real but $\rho$ is not realizable by a representation over a real vector space. Such representations will be called quaternionic (or type 3 or symplectic).

Let $\nu(\chi) = \frac{1}{|H|} \sum_{h \in H} \chi(h^2)$. The quantity $\nu(\chi)$ is called the Frobenius-Schur indicator of $\rho$.

We denote the contragredient of a representation $\pi$ by $\pi^*$.

Lemma 2.4. Let $\pi$ denote an irreducible representation of $G$. If $\pi \cong \pi^*$ then $\pi$ is real. If $\pi = \theta_{\rho,\mu}$ then $\pi$ is real if and only if $\mu$ is self-dual.
\textbf{proof:} This lemma is proven by calculating the Frobenius-Schur indicator of a representation of a generalized symmetric group.

Let $G = C^n_t \rtimes S_n$. Note that if $x = (g, \zeta), y = (h, \zeta') \in G$ then

$$x^2 = (g^2, \zeta + g(\zeta)), \quad y^{-1} = (h^{-1}, -h^{-1}(\zeta')).$$

The trace of $\theta_{\rho, \mu}(x^2)$ is $\frac{1}{|G|}$ times

$$\sum_{g \in G} \chi_{\rho}^a(y^{-1}x^2y)\mu^a(y^{-1}x^2y) = \sum_{h \in S_n} \sum_{\zeta' \in C^n_t} \chi_{\rho}^a(h^{-1}g^2h)\mu^a(h(\zeta) + hg(\zeta) + \zeta' - g^2h(\zeta')))$$

(3)

By orthogonality, the last sum is zero unless $\mu = \mu^{g^2h}$, where $\mu^{g^2h}$ is the character one obtains by composing $\mu$ with the permutation $g^2h : C^n_t \rightarrow C^n_t$.

If $g = 1$ then the inner sum in (3) above is only non-zero in case $h \in (S_n)_\mu$. If, in addition, $h \in (S_n)_\mu$ then the inner sum in the last term of (3) is equal to $\ell_n = |C^n_t|$.

Now let us sum (3) over all $x \in G$. First, note that

$$\sum_{\zeta' \in C^n_t} \mu(h(\zeta) + hg(\zeta)) = 0$$

unless $\mu^g = \mu^{-1}$. If $\mu^g = \mu^{-1}$ and $\mu = \mu^{g^2h}$ then $\mu^h = \mu$.

Therefore, either the sum of (3) is zero or there is an element $g_0 \in S_n$ such that $\mu^{g_0} = \mu^{-1} = \overline{\mu}$. In particular, $\theta_{\rho, \mu}$ is not complex if and only if $\mu$ is self-dual.

By Benard’s result [1], $G$ has no quaternionic representations.

The result now follows from [6], Proposition 39 in §13.2. \qed

3 Splitting fields

Let $\chi$ denote an irreducible character of a finite group $G$. Since the Schur index over $\mathbb{Q}$ of $\chi$ is equal to 1 [1], each such character is associated to a representation $\pi$ all of whose matrix coefficients belong to $\mathbb{Q}(\chi)$.

It is known that if $F$ is a field of characteristic $p > 0$ then $m_F(\chi) = 1$ (see Theorem 9.21(b) in [3]). Consequently, the results of this section may have analogs over a field of prime characteristic as well.
3.1 Key lemma
Let \( \theta_{\mu, \rho} \in G^* \) be the represenation defined in (2), where \( \rho \in ((S_n)_\mu)^* \).

Let \( K \subset \mathbb{Q}(\zeta) \) be a subfield which contains the field generated by the
values of the character of \( \theta_{\mu, \rho} \), where \( \zeta \) is a primitive \( \ell^r \) root of unity. Let
\( \Gamma_K = \text{Gal}(\mathbb{Q}(\zeta^\ell)/K) \). Note if we regard \( C_\ell \) as a subset of \( \mathbb{Q}(\zeta^\ell) \) then there is
an induced action of \( \Gamma_K \) on \( C_\ell \),

\[ \sigma : \mu \mapsto \mu^\sigma, \quad \mu \in (C_\ell)^*, \quad \sigma \in \Gamma_K, \]

where \( \mu^\sigma(z) = \mu(\sigma^{-1}(z)), \ z \in C_\ell \). This action extends to an action on
\( (C_\ell^n)^* = (C_\ell^*)^n \).

The following result may be called our “key lemma”.

**Lemma 3.1.** In the notation above, \( \sigma \in \Gamma_K \) induces an action \( \sigma^* \) on characters
given by \( \sigma^* : \theta_{\mu, \rho} \mapsto \theta_{\mu^\sigma, \rho} = \theta_{\mu^\sigma, \rho} \). In particular, \( \theta_{\mu, \rho} \cong \theta_{\mu^\sigma, \rho} \) if and only
if \( \mu \) is equivalent to \( \mu^\sigma \) under the action of \( S_n \) on \( (C_\ell^n)^* \) described in \( \S 2.2 \).

**proof:** This follows immediately from Lemma 2.1.

Let

\[ n_\mu(\tau) = |\{i \mid 1 \leq i \leq n, \ \mu_i = \tau\}|, \]

where \( \mu = (\mu_1, ..., \mu_n) \in (C_\ell^n)^* \) and \( \tau \in C_\ell^* \).

**Theorem 3.2.** The character of \( \theta_{\mu, \rho} \in G^* \) has values in \( K \) if and only if
\( n_\mu(\tau^\sigma) = n_\mu(\tau)^\sigma \), for all \( \sigma \in \Gamma_K \) and all \( \tau \in C_\ell^* \).

**proof:** We can extend the action of \( \Gamma_K \) on \((C_\ell^n)^* \) to \(((S_n)_\mu \times C_\ell^n)^* = ((S_n)_\mu)^* \times (C_\ell^n)^* \) by making it act trivially on the \((S_n)_\mu)^* \) component. Since
\( G^* \) is a union of such sets (by the construction in Lemma 2.1), we may extend
this action to obtain an action of \( \Gamma_K \) on \( G^* \).

To determine the circumstances under which (the equivalence class of)
\( \theta_{\mu, \rho} \) is invariant under each \( \sigma \in \Gamma_K \), we use the “key” Lemma 3.1. Since \( \mu \) is
equivalent to \( \mu^\sigma \) if and only if \( n_\mu(\chi) = n_\mu(\chi)^\sigma \), for all \( \sigma \in \Gamma_K \) and all \( \chi \in C_\ell^* \),
the theorem follows.

3.2 The main result
Let \( \Gamma = \text{Gal}(\mathbb{Q}(\zeta^\ell)/\mathbb{Q}) \), so \( \Gamma \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \). Let \( G = S_n \wr C_\ell \) and identify the
set \( G^* \) with the set of irreducible complex characters of \( G \). As was explained
above, \( \Gamma \) acts on the set \( G^* \). Indeed, let \( \gamma \in \Gamma \) be given by \( \gamma = \sigma_a \), in the
notation of §3.3 above, where \( a \in (\mathbb{Z}/\ell\mathbb{Z})^\times \), and let \( \mu = (\eta_{e_1}, \eta_{e_2}, \ldots, \eta_{e_n}) \), in the notation of §2.2 above. In this notation, \( \gamma \) sends \( \chi = \text{tr}(\theta_{\rho,\mu}) \) to \( \chi^\gamma = \text{tr}(\theta_{\rho,\mu^\gamma}) \), where

\[
\mu^\gamma = (\eta_{ae_1}, \eta_{ae_2}, \ldots, \eta_{ae_n}).
\]

Let \( \chi = \text{tr}(\theta_{\rho,\mu}) \) and let

\[
\text{Stab}_\Gamma(\chi) = \{ \gamma \in \Gamma \mid \chi = \chi^\gamma \}
\]

denote the stabilizer of \( \chi \) in \( \Gamma \). We conclude the following result.

**Lemma 3.3.** Let \( \chi = \text{tr}(\theta_{\rho,\mu}) \). We have

\[
\text{Stab}_\Gamma(\chi) = \{ \sigma_a \in \Gamma \mid (\eta_{ae_1}, \eta_{ae_2}, \ldots, \eta_{ae_n}) \sim (\eta_{e_1}, \eta_{e_2}, \ldots, \eta_{en}) \},
\]

where two \( n \)-tuples \( v, w \) satisfy \( v \sim w \) if and only if they belong to the same \( S_n \)-orbit.

We now “determine” the splitting field of any irreducible character of a generalized symmetric group.

**Theorem 3.4.** Let \( \chi = \text{tr}(\theta_{\rho,\mu}) \) be an irreducible character of \( G = S_n \) wr \( C_\ell \) as in §2.2. We have

\[
\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\chi)) = \text{Stab}_\Gamma(\chi).
\]

**proof:** If \( \gamma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\chi)) \) then \( \gamma(x) = x \) for all \( x \in \mathbb{Q}(\chi) \). In particular, \( \gamma(\chi(g)) = \chi(g) \) for all \( g \in G \). Thus, \( \gamma \in \text{Stab}_\Gamma(\chi) \). Conversely, if \( \gamma \in \text{Stab}_\Gamma(\chi) \) then \( \gamma \) must fix all elements in \( \mathbb{Q}(\chi) \). \( \square \)

**Theorem 3.5.** If \( K/\mathbb{Q} \) is any abelian extension then there is a generalized symmetric group \( G \) and an irreducible character \( \chi \) of \( G \) for which \( K = \mathbb{Q}(\chi) \). Moreover the Galois action on \( K \) is given by Lemma 3.1.

**proof:** From the theorem above and the Kronecker-Weber theorem, it suffices to show that each subgroup of \( \Gamma \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \) occurs as a \( \text{Stab}_\Gamma(\chi) \), for some irreducible character \( \chi \) of some generalized symmetric group \( G \).

Let \( H \subset \Gamma \) be a subgroup and let \( \{ e_1, \ldots, e_n \} \) denote integer representatives for the elements of \( H \). Let \( f : (\mathbb{Z}/\ell\mathbb{Z})^\times \to (C_\ell^\ast)^n \) denote the map defined by

\[
f(a)((\eta_{e_1}, \ldots, \eta_{e_n})) = (\eta_{ae_1}, \ldots, \eta_{ae_n}).
\]

Since, for all \( a \in (\mathbb{Z}/\ell\mathbb{Z})^\times \), \( aH = H \) if and only if \( a \in H \), we have \( f(a)((\eta_{e_1}, \ldots, \eta_{e_n})) \sim (\eta_{e_1}, \ldots, \eta_{en}) \) if and only if \( a \in (\mathbb{Z}/\ell\mathbb{Z})^\times \). This proves that for this choice of \( G \) and \( \chi \) (both depending on \( H \)), \( \text{Stab}_\Gamma(\chi) = H \). \( \square \)
Example 3.6. Let $G = S_4$ wr $C_8$, let $\rho = 1$ and let $\mu = (\mu_1, \mu_2, \mu_3, \mu_4) \in (C_8^*)^4$ be given by

\[ \mu_1(a) = a, \quad \mu_2(a) = a^2, \quad \mu_3(a) = a^3, \quad \mu_4(a) = a^6, \quad a \in C_8. \]

Let $\chi$ denote the character of $\theta_{1,\mu}$. A calculation using a program written in the MAPLE computer algebra package gives $\mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\chi)$.

Let $\zeta_8 = e^{2\pi i/8}$. The Galois group

\[ \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times = \{1, -1, 3, -3\}, \]

is order $\phi(8) = 4$ and is given by $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{1, \tau, \sigma, \sigma\tau\}$, where $\tau(a) = \overline{a} = a^{-1}$, $\sigma(a) = a^3$, for $a \in C_8$. If you think of $(\mathbb{Z}/8\mathbb{Z})^\times$ as a group of integers mod 8 then, under the above indicated isomorphism, $\tau$ corresponds to $-1$ and $\sigma$ to 3. Note $\text{Gal}(\mathbb{Q}(i\sqrt{2})/\mathbb{Q}) \cong \{1, \tau\}$ and $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(i\sqrt{2})) \cong \{1, \sigma\}$. Since $\sigma(\mu_1, \mu_2, \mu_3, \mu_4) = (\mu_3, \mu_4, \mu_1, \mu_2)$, Theorem 3.2 implies that $\theta_{1,\mu}$ may be realized over $\mathbb{Q}(i\sqrt{2})$. Thus $m_\mathbb{Q}(\chi) = 1$.

3.3 Galois action on subfields of cyclotomic fields

In this section, we make explicit the Galois action on the cyclotomic fields. Though it seems certain this material is known, I know of no reference.

Let $n$ denote a positive integer divisible by 4, let $r = \cos(2\pi/n)$, $s = \sin(2\pi/n)$, and let $d = n/4$. If $T_1(x) = x$, $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, ..., denote the Tchebycheff polynomials, defined by $\cos(n\theta) = T_n(\cos(\theta))$, then $T_4(r) = 0$.

If $\sigma_j \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is defined by $\sigma_j(\zeta_n) = \zeta_n^j$ then $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where $\sigma_j \mapsto j$.

Lemma 3.7. Assume $n$ is divisible by 4.

- $\mathbb{Q}(r)$ is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ with

\[ \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(r)) = \{1, \tau\}, \]

where $\tau$ denotes complex conjugation. Under the canonical isomorphism

\[ \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times, \]

we have

\[ \text{Gal}(\mathbb{Q}(r)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{-1\}. \]

9
• If $n$ is divisible by 8 then $r$ and $s$ are conjugate roots of $T_d$. In particular, $s \in \mathbb{Q}(r)$ and $T_d(s) = 0$.

• We have $\sigma_j(r) = T_j(r)$

• If $n \geq 4$ is a power of 2 then $T_d$ is the minimal polynomial of $\mathbb{Q}(r)$. Furthermore, in this case $r$ and $s$ can be explicitly computed using the following formulas:

$$
\cos(\pi/4) = \sqrt{2}/2, \quad \cos(\pi/8) = \sqrt{2 + \sqrt{2}/2}, \quad \cos(\pi/16) = \sqrt{2 + \sqrt{2 + \sqrt{2}/2}}, \quad ...
$$

The proof of this lemma is left to the reader.

Subfields of $\mathbb{Q}(r)$ may be obtained by replacing $r = \cos(2\pi/n)$ by $r_d = \cos(2\pi d/n)$, where $d|n$ (note $\cos(d\pi\theta) = T_{n/d}(\cos(d\theta))$).

References


Mathematics Department
US Naval Academy
Annapolis, Maryland
USA
email: wdj@usna.edu