J Algebr Comb (2006) 23: 189–195
DOI 10.1007/s10801-006-6923-7

Algebraic structure of association schemes of prime order

Akihide Hanaki · Katsuhiro Uno

Received: October 29, 2004 / Revised: October 29, 2004 / Accepted: July 25, 2005

Abstract Finite groups of prime order must be cyclic. It is natural to ask what about association schemes of prime order. In this paper, we will give an answer to this question. An association scheme of prime order is commutative, and its valencies of nontrivial relations and multiplicities of nontrivial irreducible characters are constant. Moreover, if we suppose that the minimal splitting field is an abelian extension of the field of rational numbers, then the character table is the same as that of a Schurian scheme.

Keywords Association scheme · Prime order · Cyclotomic scheme · Character

1. Introduction

The classification of finite simple groups is one of the most important result in group theory. Classification of (commutative) primitive schemes is also important. But it is difficult and even those having prime order have not been classified. In this paper, we prove that any scheme having prime order is commutative and its valencies of nontrivial relations and multiplicities of nontrivial irreducible characters are constant. Moreover, if we suppose that the minimal splitting field is an abelian extension of the field of rational numbers, then the character table is the same as that of a Schurian scheme.

We use the notations in Zieschang's book [9]. Let X be a finite set, and G a collection of nonempty subsets of $X \times X$. We say $g \in G$ a *relation* of (X, G). For a relation $g \in G$, we denote the *adjacency matrix* by σ_g. Namely, σ_g is a matrix whose rows and columns are indexed by X and its (x, y)-entry is 1 if $(x, y) \in g$ and 0 otherwise. We say that (X, G) is an *association scheme* if (1) $X \times X$ is a disjoint union of $g \in G$, (2) G contains the *trivial*

A. Hanaki (✉)
Faculty of Science, Shinshu University, Matsumoto, 390-8621, Japan
e-mail: hanaki@math.shinshu-u.ac.jp

K. Uno
Department of Mathematical Sciences, Osaka Kyoiku University, Kashiwara, Osaka, 582-8582, Japan
e-mail: uno@cc.osaka-kyoiku.ac.jp

relation $1 := \{(x, x) \mid x \in X\}$, (3) if $g \in G$, then $g^* := \{(y, x) \mid (x, y) \in g\} \in G$, and (4) for $f, g, h \in G$, there exists an integer a_{fgh} such that $\sigma_f \sigma_g = \sum_{h \in G} a_{fgh} \sigma_h$. We call $|X|$ the *order* of (X, G), and $n_g := a_{gg^*1}$ the *valency* of $g \in G$.

By the condition (4), we can define a $\mathbb{Z}$-algebra $\mathbb{Z}G := \bigoplus_{g \in G} \mathbb{Z}\sigma_g$ with the usual matrix multiplication. For a commutative ring R with the identity, we can define an R-algebra $RG := R \otimes_{\mathbb{Z}} \mathbb{Z}G$ and call this the *adjacency algebra* over R. When R contains $\mathbb{Z}$ as a subring, we regard $\mathbb{Z}G$ as a subring of RG. Especially, we consider σ_g is in RG. It is known that the adjacency algebra over a field of characteristic zero is semisimple [9, Theorem 4.1.3]. A *character* of G means the trace function of a linear representation of $\mathbb{C}G$, where $\mathbb{C}$ is the complex number field, and it is said to be *irreducible* if the representation is irreducible. We denote the set of all irreducible characters of G by Irr(G). Clearly the function $\sigma_g \mapsto n_g$ is a representation and also a character of G. We call this the *trivial character* of G, and denote it by 1_G. The map $\sigma_g \mapsto \sigma_g$ is also a representation of G, and its character γ satisfies $\gamma(\sigma_1) = |X|$ and $\gamma(\sigma_g) = 0$ for $1 \neq g \in G$. We call γ the *standard character* of G. The multiplicity of an irreducible character $\chi \in \mathrm{Irr}(G)$ in the standard character is denoted by m_χ and is simply called the *multiplicity* of χ.

The *character table* of (X, G) is the table, whose rows are indexed by $\chi \in \mathrm{Irr}(G)$ and columns are indexed by $g \in G$, with the (χ, g)-entry $\chi(\sigma_g)$. Usually, we append the multiplicity of the irreducible character to each row.

An association scheme (X, G) is said to be *commutative* if the adjacency algebra $\mathbb{Z}G$ is commutative, namely $a_{fgh} = a_{gfh}$ for all $f, g, h \in G$. Since $\mathbb{C}G$ is semisimple, this is equivalent to that $\chi(1) = 1$ for all $\chi \in \mathrm{Irr}(G)$. Two commutative schemes have the identical character tables if and only if they have the same intersection numbers a_{fgh}.

Example 1.1 (Schurian schemes). Let X be a finite set, and $\mathcal{G}$ a transitive permutation group on X. Let G be the set of orbits of $X \times X$ by the diagonal action of $\mathcal{G}$. Then (X, G) is an association scheme [2, Chap. II, Example 2.1]. We call this a *Schurian scheme*. It is well known that a Schurian scheme (X, G) with $|X| = p$, a prime, and $|G| = d + 1$ is isomorphic to the cyclotomic scheme $Cyc(p, d)$.

Let (X, G) be an association scheme such that $|X| = p$ is a prime number and $|G| = d + 1$. In Section 3, we will show that (X, G) is commutative. In Section 4, we determine the minimal splitting field for (X, G) under the assumption that the minimal splitting field is abelian. Finally, in Section 5, under the same assumption we determine the character table of (X, G) explicitly, and conclude that it is the same as that of $Cyc(p, d)$.

2. Discriminants of algebras

Let R be a principal ideal domain, and A an R-free R-algebra of finite rank. For a matrix representation $T : A \to M_n(R)$, we define the *discriminant* $d_T(A)$ of the representation T as follows. Let $\{a_1, \ldots, a_r\}$ be an R-basis of A. We put

$$d_T(A) = \det(\mathrm{Tr}(T(a_i a_j))),$$

where Tr is the usual trace of matrices. Especially, when the representation T is the regular representation, we call $d_T(A)$ the *discriminant* of A, and denote it by $d(A)$. We note that the discriminant depends on the choice of the basis. If we take an another basis $\{a'_1, \ldots, a'_r\}$, then $\det(\mathrm{Tr}(T(a'_i a'_j))) = \varepsilon^2 \det(\mathrm{Tr}(T(a_i a_j)))$ for some unit ε in R. Hence, if $R = \mathbb{Z}$, then the discriminant is uniquely determined.

If B is an R-subalgebra of A with the same rank, then B is also R-free and $d(A)$ is a divisor of $d(B)$.

For an algebraic number field K, the ring of integers $\mathcal{O}_K$ is a $\mathbb{Z}$-free $\mathbb{Z}$-algebra. Then $d(\mathcal{O}_K)$ is equal to the discriminant of the field K. So we denote it by $d(K)$.

Let (X, G) be an association scheme. The *Frame number* is defined by

$$\mathcal{F}(G) = |X|^{|G|} \frac{\prod_{g\in G} n_g}{\prod_{\chi\in \mathrm{Irr}(G)} {m_\chi}^{\chi(1)^2}}.$$

It is known that $\mathcal{F}(G)$ is a rational integer [3, 6] . In [4], the following fact is shown.

Proposition 2.1. *Let (X, G) be a commutative association scheme. Then $|d(\mathbb{Z}G)|$ is equal to the Frame number $\mathcal{F}(G)$.*

3. Commutativity

In this section, we will show that an association scheme (X, G) is commutative if $n_G = |X|$ is a prime number. The next lemma is crucial.

Lemma 3.1. *Let (X, G) be an association scheme. If $|X|$ is a prime number, then all nontrivial irreducible characters of G are algebraically conjugate. Especially, their multiplicities are constant.*

Proof: Put $p := |X|$. Let 1_G be the trivial character of G and χ a nontrivial irreducible character of G. Note that an algebraic conjugate of an irreducible character is again an irreducible character. Put Φ the sum of all algebraic conjugates of χ, and Ψ the sum of all nontrivial irreducible characters which are not algebraically conjugate to χ. Then the values of Φ and Ψ are rational integers. If Ψ is zero, then the assertion holds, so we assume that $\Psi \neq 0$.

We know that all eigenvalues of σ_g are congruent to n_g in characteristic p [5, Corollary 3.5]. So there exist rational integers u_g $(g \in G)$ such that $\Phi(\sigma_g) = \Phi(1)n_g - u_g p$. Similarly there exist rational integers v_g $(g \in G)$ such that $\Psi(\sigma_g) = \Psi(1)n_g - v_g p$.

By the orthogonality relation [9, Theorem 4.1.5], we have

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g} 1_G(\sigma_{g^*})\Phi(\sigma_g) = \sum_{g\in G} \Phi(\sigma_g) \\ &= \sum_{g\in G} (\Phi(1)n_g - u_g p) = p\left(\Phi(1) - \sum_{g\in G} u_g\right). \end{aligned}$$

So we have $\sum_{g\in G} u_g = \Phi(1)$ and similarly $\sum_{g\in G} v_g = \Psi(1)$. Again by the orthogonality relation,

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g}\Phi(\sigma_{g^*})\Psi(\sigma_g) = \sum_{g\in G} \frac{1}{n_g}(\Phi(1)n_{g^*} - u_{g^*}p)(\Psi(1)n_g - v_g p) \\ &= \sum_{g\in G} \Phi(1)\Psi(1)n_g - \sum_{g\in G}\Phi(1)v_g p - \sum_{g\in G}\Psi(1)u_{g^*}p + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2 \\ &= p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2 \\ &= -p\Phi(1)\Psi(1) + \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p^2, \end{aligned}$$

so we have

$$\Phi(1)\Psi(1) = \sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g p.$$

But $\Phi(1)\Psi(1)$ is relatively prime to p and $\sum_{g\in G}\frac{1}{n_g}u_{g^*}v_g$ is a p-integer, namely every n_g is relatively prime to p. So this is a contradiction. □

Lemma 3.2 ([*2, Theorem II.4.3*]). *If all nontrivial irreducible characters of G have the same multiplicities, then all nontrivial relations have the same valencies.*

Proof: Since the Frame number is a rational integer, the assertion holds by the same argument in the proof of [2, Theorem II.4.3]. □

If $|X|$ is a prime, then under the assumption that all nontrivial relations have the same valencies, Arad et al. showed in [1, Theorem 1.2] that (X, G) is commutative. Hence, combining Lemmas 3.1, 3.2 and their result, we have the main result in this section.

Theorem 3.3. *Let (X, G) be an association scheme. If $|X|$ is a prime number, then (X, G) is commutative. Moreover, all nontrivial irreducible characters are algebraically conjugate, and all valencies of nontrivial relations and all multiplicities of nontrivial irreducible characters are constant.*

Corollary 3.4. *If $|X|$ is a prime number p, then the Frame number $\mathcal{F}(G)$ is a p-power.*

4. Splitting fields

Bannai and Ito asked in [2, Section 2.7] whether the minimal splitting field of a commutative scheme is contained in a cyclotomic field, and this is still an open question. In this section, we suppose it, and determine the minimal splitting fields explicitly. For the theory of algebraic number fields, see [8], for example.

We fix a prime number p. Let (X, G) be an association scheme with $|X| = p$ and $|G| = d + 1$. Let K be the minimal splitting field of (X, G), namely

$K = \mathbb{Q}(\chi(\sigma_g) \mid \chi \in \mathrm{Irr}(G),\ g \in G)$. By Lemma 3.1, the Galois group $Gal(K/\mathbb{Q})$ acts on $\mathrm{Irr}(G) \setminus \{1_G\}$ transitively. By the Wedderburn's theorem, $\mathbb{Q}G$ is isomorphic to a direct sum of the full matrix algebras over some division rings. However, since $\mathbb{Q}G$ is commutative in our case, it is a direct sum of field extensions of $\mathbb{Q}$. Finally, since each direct summand corresponds to a $Gal(K/\mathbb{Q})$-orbit of $\mathrm{Irr}(G)$, we have

$$\mathbb{Q}G \cong \mathbb{Q} \oplus K'$$

as a $\mathbb{Q}$-algebra for some field K'. Clearly we have $\dim_{\mathbb{Q}} K' = d$. The projection $\mathbb{Q}G \to K'$ is given by a nontrivial irreducible character of G. So we can regard K' as a subfield of K. Then K is generated by K' and its algebraic conjugates.

We can say that $\mathbb{Z}G$ is a $\mathbb{Z}$-subalgebra of $\mathbb{Z} \oplus \mathcal{O}_{K'}$ in the above decomposition. The discriminant $d(\mathbb{Z} \oplus \mathcal{O}_{K'})$ is equal to the discriminant $d(K')$ of the algebraic number field K'. By Proposition 2.1, $|d(\mathbb{Z}G)|$ is the Frame number $\mathcal{F}(G)$, and it is a p-power by Corollary 3.4. So we can say that $|d(K')|$ is also a p-power, and so is $|d(K)|$ by [8, Corollary 2 to Theorem 4.25].

From here, we suppose that K is an abelian extension of $\mathbb{Q}$. Then $K = K'$. By Kronecker-Weber's theorem [8, Theorem 6.18], K is a subfield of some cyclotomic field. Let N be the conductor of K, namely N is the smallest positive integer such that K is a subfield of $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity. It is known that a prime number ℓ ramifies in $K/\mathbb{Q}$ if and only if ℓ is a divisor of N [8, Proposition 8.1]. Also ℓ ramifies in $K/\mathbb{Q}$ if and only if ℓ is a divisor of $|d(K)|$ [8, Corollary 3 of Theorem 4.24]. So we can say that $N = p^a$ for some non-negative integer a. Then, since $Gal(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$ has the unique subgroup of index d, we can say that $N = p$ and we have the following.

Theorem 4.1. *Let (X, G) be an association scheme with $|X| = p$ and $|G| = d + 1$. Suppose that the minimal splitting field K of G is an abelian extension of $\mathbb{Q}$. Then K is the unique subfield of $\mathbb{Q}(\zeta_p)$ with $\dim_{\mathbb{Q}} K = d$ and $Gal(K/\mathbb{Q})$ is a cyclic group of order d.*

Remark

(1) If we suppose $K = K'$ in the above notation, then we can also say the same conclusion in Theorem 4.1.

(2) There exists a p-Eisenstein polynomial $f(x)$ of degree d such that $K' \cong \mathbb{Q}[x]/(f(x))$, and we can say that $|d(K')| = p^{d-1}$. We know no such non-abelian field.

(3) In [7], Munemasa showed that, if all Krein parameters are rational numbers, then the minimal splitting field is abelian.

5. The character table

In this section, we determine the character table of an association schemes of prime order under the same assumption in Section 4. Then we can conclude that it is the same as that of a Schurian scheme.

Let (X, G) be an association scheme such that $|X| = p$ is a prime number and $|G| = d + 1$. Put $k := (p - 1)/d$. Suppose that the minimal splitting field K of G is an abelian extension of $\mathbb{Q}$. Let ζ_p be a primitive p-th root of unity. Then K is the unique subfield of $\mathbb{Q}(\zeta_p)$

with $\dim_{\mathbb{Q}} K = d$ by Theorem 4.1. Put $\alpha := \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$, and let τ be a generator of the cyclic group $Gal(K/\mathbb{Q})$. It is well known that $\{\alpha^{\tau^i} \mid i = 0, 1, \ldots, d-1\}$ is an integral basis of $\mathcal{O}_K$.

Firstly, we describe the character table of the cyclotomic scheme $Cyc(p, d)$ without a proof.

Lemma 5.1. *The character table of* $Cyc(p, d)$ *is as follows.*

1	1	k	k	$\cdots$	k	1
φ	1	α	α^{τ}	$\cdots$	$\alpha^{\tau^{d-1}}$	k
φ^{τ}	1	α^{τ}	α^{τ^2}	$\cdots$	α	k
		$\cdots$	$\cdots$	$\cdots$		
$\varphi^{\tau^{d-1}}$	1	$\alpha^{\tau^{d-1}}$	α	$\cdots$	$\alpha^{\tau^{d-2}}$	k

By the second orthogonality relations [2, Theorem II.3.5 (iii)] for the cyclotomic scheme, we have the next easy lemma.

Lemma 5.2. *Use the above notations, then we have* $\sum_{i=0}^{d-1} \alpha^{\tau^i} = -1$ *and*

$$\sum_{i=0}^{d-1} \alpha^{\tau^i} \overline{\alpha}^{\tau^{i+j}} = \begin{cases} p-k & \textit{if } j \equiv 0 \pmod{d}, \\ 0 & \textit{otherwise}. \end{cases}$$

Now we consider the character table of (X, G). By Lemma 3.1, it looks like the following.

	1	g_1	g_2		g_d	
1_G	1	k	k	$\cdots$	k	1
χ	1	β_1	β_2	$\cdots$	β_d	k
χ^{τ}	1	β_1^{τ}	β_2^{τ}	$\cdots$	β_d^{τ}	k
		$\cdots$	$\cdots$	$\cdots$		
$\chi^{\tau^{d-1}}$	1	$\beta_1^{\tau^{d-1}}$	$\beta_2^{\tau^{d-1}}$	$\cdots$	$\beta_d^{\tau^{d-1}}$	k

We fix $g_j \in G$ for a while. Since $\{\alpha^{\tau^i} \mid i = 0, 1, \ldots, d-1\}$ is an integral basis of $\mathcal{O}_K$ and $\beta_j \in \mathcal{O}_K$, there exist $b_s \in \mathbb{Z}$ such that

$$\beta_j = \sum_{s=0}^{d-1} b_s \alpha^{\tau^s}.$$

By the second orthogonality relation with respect to g_j and 1, we have

$$0 = k\left(1 + \sum_{i=0}^{d-1} \beta_j^{\tau^i}\right) = k\left(1 + \sum_{i=0}^{d-1} \sum_{s=0}^{d-1} b_s \alpha^{\tau^{i+s}}\right) = k\left(1 - \sum_{s=0}^{d-1} b_s\right)$$

by Lemma 5.2. So we have $\sum_{s=0}^{d-1} b_s = 1$. Again by the second orthogonality relation with respect to g_j and itself, we have

$$\begin{aligned} pk &= k\left(k + \sum_{i=0}^{d-1} \beta_j^{\tau^i} \overline{\beta_j}^{\tau^i}\right) = k\left(k + \sum_{i=0}^{d-1}\sum_{s=0}^{d-1}\sum_{t=0}^{d-1} b_s b_t \alpha^{\tau^{i+s}} \overline{\alpha}^{\tau^{i+t}}\right) \\ &= k\left(k + (p-k)\sum_{s=0}^{d-1} b_s^2\right) \end{aligned}$$

by Lemma 5.2. This means $\sum_{s=0}^{d-1} b_s^2 = 1$, and consequently we have that the only one $b_s = 1$ and the others are zero. Namely, $\beta_j = \alpha^{\tau^s}$ for some $0 \leq s < d$.

The character table does not have the identical columns. This shows that the character table of (X, G) is the same as that of $Cyc(p, d)$ by a suitable reordering of G. Now we have the main result.

Theorem 5.3. *Let (X, G) be an association scheme of prime order p with $|G| = d + 1$. Suppose that the minimal splitting field of G is an abelian extension of $\mathbb{Q}$. Then the character table of (X, G) is the same as that of the cyclotomic scheme $Cyc(p, d)$.*

Acknowledgments The authors are very grateful to Hanguk Kang who pointed out an incorrect part in the earlier version of this paper.

References

1. Z. Arad, E. Fisman, and M. Muzychuk, “Generalized table algebras,” *Israel J. Math.* **114** (1999), 29–60.
2. E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin-Cummings, Menlo Park CA, 1984.
3. J.S. Frame, “The double cosets of a finite group,” *Bull. Amer. Math. Soc.* **47** (1941), 458–467.
4. A. Hanaki, “Semisimplicity of adjacency algebras of association schemes,” *J. Algebra* **225** (2000), 124–129.
5. A. Hanaki, “Locality of a modular adjacency algebra of an association scheme of prime power order,” *Arch. Math.* **79** (2002), 167–170.
6. D. G. Higman, “Schur relations for weighted adjacency algebras,” *Symp. Math. Roma* (London-New York), **13** (1974), 467–477.
7. A. Munemasa, “Splitting fields of association schemes,” *J. Combin. Theory. Ser. A* **57** (1991), 157–161.
8. W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd Edition, Springer-Verlag, Berlin, Heidelberg, New York, 2004.
9. P.-H. Zieschang, “An algebraic approach to association schemes,” Lecture Notes in Mathematics, 1628, Springer-Verlag, Berlin, 1996.