GROUP ALGEBRAS

The aim of this note is to demonstrate how to give a quiver with relations for a given finite dimensional algebra. In particular, we will deal with group algebras for example. However, we do not give details in this note. The reader should follow them up.

Throughout this note, let k be an algebraically closed field of characteristic p and G a finite group. Note that p is a prime or zero. The order of G is denoted by $|G|$.

We always mean by an algebra and a module a finite dimensional k-algebra and a finite dimensional right module, respectively.

1. THE CASE THAT p DOES NOT DIVIDE $|G|$

This section is devoted to studying a well-known result on semisimple group algebras.

A *semisimple algebra* is an algebra which is semisimple as a module, that is, it is a direct sum of simple modules.

A crucial fact on semisimple algebras is Wedderburn-Artin's theorem; e.g. [DK, Theorem 2.4.3]. We leave the proof to the reader.

Theorem 1 (Wedderburn-Artin)**.** *Every semisimple algebra is isomorphic to a direct product of matrix algebras over k, and the converse also holds.*

Observe that the matrix algebra $M_n(k)$ with size n has only one simple module S up to isomorphism, whose dimension is just n. Moreover, the algebra can be written by a direct sum of n copies of S as a module, i.e. $M_n(k) \simeq nS$; e.g. [DK, Proposition 2.3.4].

This observation leads us to the following conclusion.

Corollary 2. *Any semisimple algebra decomposes into the form $n_1S_1 \oplus n_2S_2 \oplus \cdots \oplus n_\ell S_\ell$, where S_i's are pairwise non-isomorphic simple modules with dimension n_i.*

Now, we state a main theorem of this section; e.g. [A, I, 3, Theorem 1].

Theorem 3. *The algebra kG is semisimple if and only if p does not divide $|G|$.*

Proof. Suppose that p divides $|G|$. We define an ideal J of kG by

$$J := \left\{ \sum_{g\in G} \alpha_g g \;\middle|\; \sum_{g\in G} \alpha_g = 0 \right\}.$$

(Check that this is exactly an ideal of kG.) Recall that the *trivial module* V is a kG-module which is k as a vector space and has a trivial action, that is, for $\alpha \in V$ and $g \in G$ $\alpha g = \alpha$. Then, we see that the homomorphism $\varphi : kG \to V$ defined by $\displaystyle\sum_{g\in G}\alpha_g g \mapsto \sum_{g\in G}\alpha_g$ has kernel J. (Check!) Hence, it follows from homomorphism theorem that kG/J is isomorphic to V.

Date: November 25, 2016.

Written by Takuma Aihara.

On the other hand, let S be a subspace of kG spaned by $\sigma := \sum_{g\in G} g$. As $\sigma \cdot h = \sigma$ for any element h of G, S becomes a kG-module which is isomphic to the trivial module V. Moreover, we observe that S is contained in J by $p \mid |G|$.

Thus, we have a composition series $kG \supseteq J \supseteq S \supseteq 0$ of kG, in which the trivial module appears twice. By $\dim V = 1$ and Corollary 2, this does not occur in the case that kG is semisimple.

Assume that p does not divide $|G|$. We show that any submodule N of a kG-module M is its direct summand: If proved, then every kG-module, and also kG itself, is semisimple. Since N is a direct summand of M as a vector space, we have a projection $\pi : M \to N$ of a vector space. Define $\pi' : M \to N$ by

$$m \mapsto \frac{1}{|G|}\sum_{g\in G} \pi(mg)g^{-1}.$$

Note that this is definable, since $|G|$ is invertible in k by $p \nmid |G|$. For $m \in M$ and $h \in G$, we obtain

$$\pi'(mh) = \frac{1}{|G|}\sum_{g\in G} \pi(mhg)g^{-1} = \frac{1}{|G|}\sum_{g'=hg} \pi(mg')g'^{-1} \cdot h = \pi'(m)h,$$

whence π' is a homomorphism. Moreover, one observes $\pi'(n) = n$ for $n \in N$ by $\pi(n) = n$. By [DK, Proposition 1.6.2], it finds out that N is a direct summand of M. □

By Theorem 3, we obtain a quiver with relations of a group algebra in the case of $p \nmid |G|$, which has n vertices and no arrow, where n denotes the number of simple modules. So, we have only to give a central decomposition of the identity of kG with minimal (primitive) idempotents. To do this, we need the notion and the knowledge of the ordinary representation of finite groups; e.g. [NT]. In particular, it is convenient to use ordinary character tables: They will be put in each section, but we will not give any more details about them. (See [NT, III, §1,2 and Theorem 2.22].)

2. Order 2

In this section, we give quivers with relations of kG, where G is the cyclic group C_2 of order 2. Let $G = \langle g \mid g^2 = 1\rangle$.

The ordinary character table of G is the following:

	1	g
χ_1	1	1
χ_2	1	-1

2.1. char $k \neq 2$.

In this case, kG is semisimple by Theorem 3.

Note that the integer 2 is invertible in k by $\operatorname{char} k \neq 2$. So, we put

$$e_1 = \frac{1}{2}(1+g) \text{ and } e_2 = \frac{1}{2}(1-g).$$

One can easily check that these give a central decomposition of the identity with minimal idempotents. So, we are done.

2.2. $\operatorname{char} k = 2$.

We observe that the identity is a minimal idempotent. Putting

$$x := 1 - g,$$

one has $x^2 = 0$. Now, it is not difficult to check that kG is isomorphic to the algebra presented by the quiver

with relation $x^2 = 0$. Thus, we get the quiver with relations of kG.

3. Order 3

We consider the cyclic group C_3 of order 3 and let $G = \langle g \mid g^3 = 1 \rangle$.

3.1. $\operatorname{char} k \neq 3$.

It follows from Theorem 3 that kG is semisimple.

Let ω be a primitive 3rd root of the identity, that is, $\omega^3 = 1$ and $\omega^i \neq 1$ for any $i = 1, 2$. We give the ordinary character table of G:

	1	g	g^2
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

Then, we put

$$e_1 = \frac{1}{3}(1 + g + g^2),\ e_2 = \frac{1}{3}(1 + \omega g + \omega^2 g^2) \text{ and } e_3 = \frac{1}{3}(1 + \omega^2 g + \omega g^2).$$

It is observed that these give a central decomposition of the identity with minimal idempotents. Thus, it is completed.

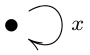
3.2. $\operatorname{char} k = 3$.

In this case, the identity is a minimal idempotent.

Putting

$$x := 1 - g,$$

we can easily check that kG is isomorphic to the algebra given by the quiver



with relation $x^3 = 0$. Thus, we are done.

4. Order 4

In this case, there are two groups up to isomorphism: One is the cyclic group C_4 and the other is the elementary abelian group $C_2 \times C_2$.

4.1. **The cyclic group.**

Let $G = \langle g \mid g^4 = 1 \rangle$.

4.1.1. char $k \neq 2$. Let ω be a primitive 4th root of the identity.

The ordinary character table of G is:

	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	ω	ω^2	ω^3
χ_3	1	ω^2	ω^3	ω
χ_4	1	ω^3	ω	ω^2

Put

$$e_1 = \frac{1}{4}(1 + g + g^2 + g^3), \qquad e_2 = \frac{1}{4}(1 + \omega g + \omega^2 g^2 + \omega^3 g^3),$$

$$e_3 = \frac{1}{4}(1 + \omega^2 g + \omega^3 g^2 + \omega g^3) \text{ and } e_4 = \frac{1}{4}(1 + \omega^3 g + \omega g^2 + \omega^2 g^3).$$

Check that these are the desired idempotents.

4.1.2. char $k = 2$. Putting

$$x := 1 - g,$$

observe that kG is isomorphic to the algebra presented by the quiver

with relation $x^4 = 0$.

4.2. **The elementary abelian group.** Let $G = \langle a, b \mid a^2 = b^2 = 1,\ ba = ab \rangle$.

We give the ordinary character table of G:

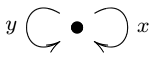
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

4.2.1. char $k \neq 2$. Show that the sum $1 = e_1 + e_2 + e_3 + e_4$ is a central decomposition of the identity with minimal idempotents, where e_1, e_2, e_3 and e_4 are the following:

$$e_1 = \frac{1}{4}(1 + a + b + ab), \qquad e_2 = \frac{1}{4}(1 + a - b - ab),$$

$$e_3 = \frac{1}{4}(1 - a + b - ab) \text{ and } e_4 = \frac{1}{4}(1 - a - b + ab).$$

4.2.2. char $k = 2$. Show that kG is isomorphic to the algebra given by the quiver



with relations $x^2 = 0 = y^2$ and $yx = xy$, where $x := 1 - a$ and $y := 1 - b$.

5. Order 5

We give the quiver with relations of kG, where G is the cyclic group of order 5. Let $G = \langle g \mid g^5 = 1 \rangle$.

5.1. $\operatorname{char} k \neq 5$.

Let ω be a primitive 5th roof of the identity and put

$$e_1 = \frac{1}{5}(1 + g + g^2 + g^3 + g^4), \qquad e_2 = \frac{1}{5}(1 + \omega g + \omega^2 g^2 + \omega^3 g^3 + \omega^4 g^4),$$
$$e_3 = \frac{1}{5}(1 + \omega^2 g + \omega^3 g^2 + \omega^4 g^3 + \omega g^4), \quad e_4 = \frac{1}{5}(1 + \omega^3 g + \omega^4 g^2 + \omega g^3 + \omega^2 g^4)$$

and

$$e_5 = \frac{1}{5}(1 + \omega^4 g + \omega g^2 + \omega^2 g^3 + \omega^3 g^4).$$

Here, we give the ordinary character table of G:

	1	g	g^2	g^3	g^4
χ_1	1	1	1	1	1
χ_2	1	ω	ω^2	ω^3	ω^4
χ_3	1	ω^2	ω^3	ω^4	ω
χ_4	1	ω^3	ω^4	ω	ω
χ_5	1	ω^4	ω	ω^2	ω^3

Now, we are done.

5.2. $\operatorname{char} k = 5$.

The identity is a minimal idempotent and the algebra kG is given by

with relation $x^5 = 0$, where $x := 1 - g$.

6. Order 6

There exist two groups with order 6 up to isomorphism: One is the cyclic group C_6 and the dihedral group D_6.

6.1. **The cyclic group.**

Let $G = \langle g \mid g^6 = 1 \rangle$.

6.1.1. $\operatorname{char} k \neq 2, 3$.

Let ω be a primitive 6th root of the identity.

The ordinary character table of G is the following:

	1	g	g^2	g^3	g^4	g^5
χ_1	1	1	1	1	1	1
χ_2	1	ω	ω^2	ω^3	ω^4	ω^5
χ_3	1	ω^2	ω^3	ω^4	ω^5	ω
χ_4	1	ω^3	ω^4	ω^5	ω	ω^2
χ_5	1	ω^4	ω^5	ω	ω^2	ω^3
χ_6	1	ω^5	ω	ω^2	ω^3	ω^4

Minimal idempotents appearing in a central decomposition of the identity are the following:

$$e_1 = \frac{1}{6}(1+g+g^2+g^3+g^4+g^5), \qquad e_2 = \frac{1}{6}(1+\omega g+\omega^2 g^2+\omega^3 g^3+\omega^4 g^4+\omega^5 g^5),$$

$$e_3 = \frac{1}{6}(1+\omega^2 g+\omega^3 g^2+\omega^4 g^3+\omega^5 g^4+\omega g^5), \quad e_4 = \frac{1}{6}(1+\omega^3 g+\omega^4 g^2+\omega^5 g^3+\omega g^4+\omega^2 g^5),$$

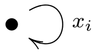
$$e_5 = \frac{1}{6}(1+\omega^4 g+\omega^5 g^2+\omega g^3+\omega^2 g^4+\omega^3 g^5), \quad e_6 = \frac{1}{6}(1+\omega^5 g+\omega g^2+\omega^2 g^3+\omega^3 g^4+\omega^4 g^5).$$

6.1.2. char $k = 2$. Let ω be a primitive 3rd root of the identity and put

$$e_1 = \frac{1}{3}(1+g^2+g^4), \ e_2 = \frac{1}{3}(1+\omega g^2+\omega^2 g^4) \text{ and } e_3 = \frac{1}{3}(1+\omega^2 g^2+\omega g^4).$$

These give a central decomposition of the identity with minimal idempotents. Hence, we see that $\Lambda := kG$ is isomorphic to a direct product of three algebras by [DK, Theorem 1.7.7], namely, $\Lambda_1 = e_1\Lambda e_1, \Lambda_2 = e_2\Lambda e_2$ and $\Lambda_3 := e_3\Lambda e_3$.

Setting $x := 1 - g^3$, prove that Λ_i is the algebra presented by the quiver



with relation $x_i^2 = 0$, where $x_i := e_i x$ and the vertex corresponds to e_i.

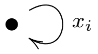
6.1.3. char $k = 3$. We modify the case of char $k = 2$ as follows.

Minimal idempotents

$$e_1 = \frac{1}{2}(1+g^3) \text{ and } e_2 = \frac{1}{2}(1-g^3)$$

give a central decomposition of the identity, whence $\Lambda := kG \simeq e_1\Lambda e_1 \times e_2\Lambda e_2$.

The algebra $e_i\Lambda e_i$ figures out to be given by



with relation $x_i^3 = 0$, where $x_i := e_i(1-g^2)$ and the vertex corresponds to e_i.

6.2. **The dihedral group.** Let $G = \langle a, b \mid a^3 = b^2 = 1, \ ba = a^2 b\rangle$.

We give the ordinary character table of G:

	1	a, a^2	b, ab, a^2b
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

6.2.1. char $k \neq 2, 3$. Find a central decomposition $1 = e_1 + e_2 + e_3$ of the identity with minimal idempotents:

$$e_1 = \frac{1}{6}(1+a+a^2+b+ab+a^2b), \ e_2 = \frac{1}{6}(1+a+a^2-b-ab-a^2b)$$

and

$$e_3 = \frac{2}{6}(2-a-a^2).$$

Note that $e_3\Lambda e_3$ is isomorphic to the matrix algebra $M_2(k)$.

6.2.2. $\operatorname{char} k = 2$. Minimal idempotents

$$e_1 = \frac{1}{3}(1 + a + a^2) \text{ and } e_2 = \frac{1}{3}(2 - a - a^2)$$

give a central decomposition of the identity, whence $\Lambda = kG \simeq e_1\Lambda e_1 \times e_2\Lambda e_2$.

The algebra $e_1\Lambda e_1$ is presented by the quiver

$$\begin{tikzcd}\bullet \arrow[loop right, "x_1"]\end{tikzcd}$$

with relation $x_1^2 = 0$, where $x_1 := e_1(1 - b)$ and the vertex corresponds to e_1.

The algebra $e_2\Lambda e_2$ is isomorphic to the matrix algebra $M_2(k)$.

6.2.3. $\operatorname{char} k = 3$. Putting

$$e_1 = \frac{1}{2}(1 + b) \text{ and } e_2 = \frac{1}{2}(1 - b),$$

it is obtained that $1 = e_1 + e_2$ is a decomposition of the identity. Let $x := e_1(1 - a)e_2$ and $y := e_2(1 - a)e_1$. Then, we see that kG is isomorphic to the algebra presented by the quiver

$$\begin{tikzcd}1 \arrow[r, shift left, "x"] & 2 \arrow[l, shift left, "y"]\end{tikzcd}$$

with relations $xyx = 0 = yxy$, where the vertices 1 and 2 correspond to e_1 and e_2, respectively.

Appendix A. p-groups

In this appendix, we study group algebras of p-groups, which are groundwork for the modular representation theory of finite groups.

Recall that we have set $p = \operatorname{char} k$ and G as a finite group.

In the rest of this appendix, we assume that p divides the order of G, which implies that kG is not semisimple by Theorem 3.

We would like to show the following important result.

Theorem 4. *The group algebra of any p-group G admits precisely one simple module, which is the trivial kG-module.*

Before giving a proof of this theorem, let us recall fundamental facts of linear algebras and groups: We leave their proofs to the reader.

We treat all numerical vectors as row ones, and hence the matrix algebra naturally acts from right hand side. The identity matrix is denoted by E.

Let X be a matrix with size d. An *eigen value* λ in k and *eigen vector* v in k^d of X are defined to satisfy $vX = \lambda v$. To find eigen values, we consider the *characteristic polynomial* $F_X(x) := \det(xE - X)$ with a variable x and solve the *characteristic equation* $F_X(x) = 0$. Here, det stands for the determinant of a matrix. Note that any characterstic equation absolutely has a root since the base field k is algebraically closed. For an eigen value λ of X, the *eigen space* W consists of all eigen vectors corresponding to λ:

$$W = \{v \in k^d \mid vX = \lambda v\}.$$

For a polynomial $f(x) = \sum_{i=0}^{d} \alpha_i x^i$ with a variable x, we substitute X for $f(x)$ by $f(X) = \sum_{i=0}^{d} \alpha_i X^i$. Here, we regard X^0 as E. The *minimal polynomial* $m_X(x)$ of X is the polynomial of the least degree with the leading coefficient 1 that has X as a root.

An important fact is the following:

Fact 5. *Let X be a matrix. Then the following hold:*

1. *If a polynomial $f(x)$ satisfies $f(X) = 0$, then the minimal polynomial $m_X(x)$ divides $f(x)$.*
2. *Every eigen value of X is a root of $m_X(x) = 0$.*

We also recall a basic fact on p-groups.

Fact 6. *The center of any p-group has an element other than the identity.*

Now, we are ready to prove Theorem 4.

Proof of Theorem 4. We know that every group algebra has the trivial module, and so one should prove that a simple kG-module V is just the trivial one. Let T be the corresponding matrix representation of V.

We first show that the matrix $X := T_g$ has 1 as an eigen value for any element g of G. Putting $|G| = p^n$, we oberve $X^{p^n} = E$. Taking into account $p = \operatorname{char} k$, one has $0 = E - X^{p^n} = (E - X)^{p^n}$. By Fact 5, the minimal polynomial of X divides $(1 - x)^{p^n}$, whence 1 is an eigen value of X.

Thus, for every element g of G the eigen space W_g corresponding to the eigen value 1 is a non-zero subspace of V:

$$W_g = \{v \in V \mid vg = v\}.$$

(For this, consider the canonical isomorphism $\operatorname{End}_k(V) \simeq M_d(k)$ by $V \simeq k^d$ as a vector space, where $d = \dim V$.)

We show that W_g becomes a submodule of V if g lies in the center $Z(G)$ of G, that is, for any $h \in G$ and $w \in W_g$, $wh \in W_g$. By $wg = w$ and $gh = hg$, we obtain equalities

$$(wh)g = (wg)h = wh,$$

which implies that wh belongs to W_g.

Finally, we show that V is isomorphic to the trivial module. To do this, one has to check $vg = v$ for any $v \in V$ and $g \in G$, and $\dim V = 1$. Since W_g is a non-zero submodule of a simple module V, they find out to coincide. Now, we use induction on the order p^n of G. Since G is a p-group, we see from Fact 6 that the center $Z := Z(G)$ of G has an element $z \neq 1$ and the order of the quotient group G/Z is strictly smaller than that of G. By the induction hypothesis, it is obtained that $k[G/Z]$ admits only one simple module, which is the trivial one. As $V = W_z$, observe that it also becomes a simple $k[G/Z]$-module by $v(gZ) := vg$: To do this, we have to check that this action is well-defined and that V is also simple as a $k[G/Z]$-module. Hence, V is the trivial module over $k[G/Z]$, from which we get $vg = v$ and $\dim V = 1$. □

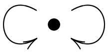
We denote by $D(G)$ the derived subgroup of G, which is generated by $ghg^{-1}h^{-1}$ for all elements g and h of G. It is well-known that $D(G)$ is the smallest normal subgroup of G

such that the quotient group is abelian. Therefore, we can write $G/D(G) \simeq C_{\ell_1} \times \cdots \times C_{\ell_m}$ with $\ell_{i+1} \mid \ell_i$. Then the *p-rank* of G is the number of $\ell_i' s$ satisfying $p \mid \ell_i$. By $\ell_{i+1} \mid \ell_i$, it is the greatest non-negative integer r with $p \nmid \ell_{r+1}$.

We close this note by giving a useful result and examples on loops at the vertex corresponding to the trivial module.

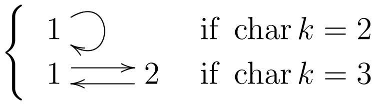
Theorem 7 ('cite'). *Let kG be presented by a quiver Q and relations. Let t be the vertex of Q corresponding to the trivial module of kG. Then the number of loops at t is equal to the p-rank of G.*

For example, let G be the elementary abelian group $C_2 \times C_2$ of order 4 and $p = 2$. By Theorem 4, we observe that kG has only one simple module, and so the quiver admits precisely one vertex. It is evident that the 2-rank of G is 2, and we have already seen that the quiver is given by



Thus, it is obtained that the 2-rank of the group and the number of loops coincide.

Let G be the dihedral group D_6 of order 6. By $D(G) = \langle a \rangle$ and $G/D(G) \simeq C_2$, the 2- and 3-ranks of G are 1 and 0, respectively. On the other hand, the quivers of kG are



where the vertex 1 corresponds to the trivial module. This also says that the 2- or 3-rank of the group coincides with the number of loops.

References

[A] J. L. Alperin, Local representation theory. Cambridge Studies in Advanced Mathematics, **11**. *Cambridge University Press, Cambridge*, 1986.

[DK] Y. A. drozd and V. V. Kirichenko, Finite dimensional algebras. *Springer-Verlag, Berlin*, 1994.

[NT] 永尾汎, 津島行男, 有限群の表現論. 裳華房, 1987.