



Math 5555

Abstract Algebra II

Book 3

For each $i \in \{1, 2, \dots, k\}$, we solve n_i equations (one for each $t \in \{1, \dots, n_i\}$)

in n_i unknowns $\lambda_{i,j}$, $j \in \{1, 2, \dots, n_i\}$.

In general the n_i symmetric polynomials $\lambda_{i,1}^t + \dots + \lambda_{i,n_i}^t$, $1 \leq t \leq n_i$, can be re-expressed in terms of the elementary symmetric polynomials $e_j = e_j(\lambda_{i,1}, \dots, \lambda_{i,n_i})$ which are the coefficients of

Use
(Newton's identities)

$$(x + \lambda_{i,1})(x + \lambda_{i,2}) \dots (x + \lambda_{i,n_i}) = x^{n_i} + e_1 x^{n_i-1} + e_2 x^{n_i-2} + \dots + e_{n_i} x + e_{n_i}$$

i.e. $e_0 = \lambda_{i,1} \lambda_{i,2} \dots \lambda_{i,n_i}$

$$e_2 = \sum \lambda_{i,r} \lambda_{i,s}$$

$$e_1 = \lambda_{i,1} + \dots + \lambda_{i,n_i}$$

We will show: if $|G| = n$ then $\mathbb{C}G \cong \bigoplus_{i=1}^k M(n_i, \mathbb{C})$ (algebra isomorphism)

where $k =$ number of conjugacy classes in G .

The center of R (semisimple algebra) is $Z(R) = \{z \in R : zx = xz \text{ for all } x \in R\}$.

$M(n, \mathbb{C}) = \{n \times n \text{ complex matrices}\}$

$Z(R) \subseteq R$ is a subalgebra: a subspace which is also a subring.

$Z(M(n, \mathbb{C})) = \{\lambda I : \lambda \in \mathbb{C}\}$

$$I = I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}_{n \times n}$$

$$Z\left(\bigoplus_{i=1}^k M(n_i, \mathbb{C})\right) = Z\left(\begin{bmatrix} * & & & 0 \\ * & n_2 \times n_2 & & \\ & * & & \\ 0 & & * & n_k \times n_k \end{bmatrix}\right) = \left\{ \begin{bmatrix} \lambda_1 I_{n_1} & & & 0 \\ & \lambda_2 I_{n_2} & & \\ & & \ddots & \\ 0 & & & \lambda_k I_{n_k} \end{bmatrix} : \lambda_1, \dots, \lambda_k \in \mathbb{C} \right\}$$

$$\dim \bigoplus_{i=1}^k M(n_i, \mathbb{C}) = \sum_{i=1}^k n_i^2 ; \quad \dim \left(Z\left(\bigoplus_{i=1}^k M(n_i, \mathbb{C})\right) \right) = k$$

$$\dim \mathbb{C}G = n = |G|$$

$$\dim \mathbb{Z}(CG) = k = \text{no. of conj. classes.}$$

Let $K_1, \dots, K_k \subset G$ be the conj. classes i.e. $G = K_1 \sqcup K_2 \sqcup \dots \sqcup K_k$

For $1 \leq i \leq k$, let $z_i = \sum_{g \in K_i} g = \text{sum of elements in } K_i$

$$z_i \in \mathbb{Z}(CG) \text{ because } \begin{aligned} gz_i &= z_i g \\ gz_i g^{-1} &= z_i \end{aligned}$$

$$\mathbb{Z}(CG) = \left\{ a_1 z_1 + \dots + a_k z_k : a_i \in \mathbb{C} \right\}$$

Given $z \in \mathbb{Z}(CG)$, say $z = \sum_{x \in G} a_x x \quad a_x \in \mathbb{C}$

For all $g \in G$, $\begin{aligned} gz &= zg \\ gzg^{-1} &= z \end{aligned}$

$$\mathbb{Z}G = \text{integral group ring of } G = \left\{ \sum_{g \in G} a_g g : a_g \in \mathbb{Z} \right\}$$

$$\mathbb{Q}G = \text{rational group algebra} \quad \dots \quad \mathbb{Q}$$

$$\mathbb{R}G = \text{real group algebra} \quad \dots \quad \mathbb{R}$$

$$FG = \text{group algebra of } G \text{ over } F \quad \dots \quad F$$

$$F[G] = FG \quad \text{when } G \text{ is a group.}$$

$F[x, y, z]$ = polynomial algebra in x, y, z with coefficients in F (infinite dimensional)
 as distinguished from $Fx + Fy + Fz = \langle x, y, z \rangle_F = \{a_x x + a_y y + a_z z : a_x, a_y, a_z \in F\}$
 which is a 3-dimensional vector space

If R is an algebra over F and $S \subseteq R$ (any subset) then
 the centralizer of S in R is

$$C_R(S) = \{z \in R : zs = sz \text{ for all } s \in S\} \subseteq R \text{ subalgebra}$$

(Also called the commutant of S in R).

$$C_R(R) = Z(R)$$

Schur's Lemma (late 19th century)

Let R be a semisimple algebra over \mathbb{C} , e.g. $R = M(n, \mathbb{C})$, or $\bigoplus_{i=1}^k M(n_i, \mathbb{C})$, or $\mathbb{C}G$, $1/G < \infty$.

Let M, N be R -^{simple} modules and $\phi : M \rightarrow N$ a homomorphism i.e. $\phi(rm + sm') = r\phi(m) + s\phi(m')$

For all $r, s \in R$; $m, m' \in M$.

(i) If $M \not\cong N$ as R -modules then $\phi = 0$.

There are no nonzero homomorphisms between simple modules.

(ii) If $M \cong N$, say $M = N$, then $\phi = cI$ for some $c \in \mathbb{C}$.

Proof (i) If $\phi \neq 0$ then there exists $v_0 \in M$ such that $\phi(v_0) \neq 0$, so $\underline{R\phi(v_0)} \subseteq \phi(M) \subseteq N$
 is a nonzero submodule of N . Since N is simple, $R\phi(v_0) = N$.

The kernel of $\phi : M \rightarrow N$ is a submodule of M .

Since M is simple $\ker \phi = 0$ or M . But $\phi \neq 0$ ($\phi(v_0) \neq 0$) we have
 $\ker \phi = 0$. By the first isomorphism theorem, $M \cong M / \ker \phi \cong \phi(M) = N$

This contradicts $M \not\cong N$.

(ii) Let $\phi: M \rightarrow M$ be a homomorphism of the simple R -module M .
 In particular ϕ is a \mathbb{C} -linear transformation of a finite dimensional complex vector space so there exists $v_0 \in M, v_0 \neq 0$ such that $\phi(v_0) = cv_0$ for some $c \in \mathbb{C}$ (\mathbb{C} is alg. closed). Let $\tilde{\phi} = \phi - cI$ so $\tilde{\phi}$ is a homomorphism of R -algebras:

$$\tilde{\phi}(rm) = \phi(rm) - cirm = r\phi(m) - crm = r(\phi(m) - cm) = r\tilde{\phi}(m)$$

$$\tilde{\phi}(m+m') = \tilde{\phi}(m) + \tilde{\phi}(m') \quad (r \in R; m, m' \in M)$$

$$v_0 \in \ker \tilde{\phi} \neq 0 \Rightarrow \ker \tilde{\phi} = M \Rightarrow \tilde{\phi} = 0 \Rightarrow \phi = cI. \quad \square$$

Remark If $M \cong N$ as R -modules there is an isomorphism $A: M \rightarrow N$
 (A invertible $n \times n$ matrix, $n = \dim M = \dim N$)
 $A(rm) = rAm$ for all $r \in R$.

then the R -module homomorphisms $M \rightarrow N$ all have the form $cA, c \in \mathbb{C}$.

The choice of field \mathbb{C} is important for Schur's lemma e.g.

$$G = \{1, g, g^2, g^3\} \text{ cyclic of order 4, } \pi: G \rightarrow GL_2(\mathbb{R})$$

$$g \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$M = \mathbb{R}^2$ is an RG -module using π

$$\pi(g) \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

π makes M into an R -module for $R = RG$

M is a simple module but the R -homomorphisms $M \rightarrow M$ are more than just
 $aI = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$; we have $\begin{bmatrix} a & b \\ b & a \end{bmatrix} \quad (a, b \in \mathbb{R})$

Recall Schur's lemma:

If $\pi: G \rightarrow GL_n(\mathbb{C})$ is an irreducible representation then the only $n \times n$ matrices commuting with $\pi(g)$, $g \in G$ are the scalar matrices λI_n ($\lambda \in \mathbb{C}$)

If π, π' are representations of, $\pi: G \rightarrow GL_m(\mathbb{C})$, $\pi': G \rightarrow GL_n(\mathbb{C})$ then π defines an action of G on \mathbb{C}^m . $g \in G$ acts on $v \in \mathbb{C}^m$ ($m \times 1$ column vector) as $gv = \pi(g)v \in \mathbb{C}^m$

and π' defines an action of G on \mathbb{C}^n , $gv = \pi'(g)v \in \mathbb{C}^n$

then a $\mathbb{C}G$ -homomorphism of the corresponding modules is (concretely) an $n \times m$ matrix $A \in \mathbb{C}^{n \times m}$: $\mathbb{C}^m \rightarrow \mathbb{C}^n$ such that

$$\begin{array}{ccc} \mathbb{C}^m & \xrightarrow{A} & \mathbb{C}^n \\ \pi(g) \downarrow & & \downarrow \pi'(g) \\ \mathbb{C}^m & \xrightarrow{A} & \mathbb{C}^n \end{array} \text{ commutes for every } g \in G \text{ i.e. } \pi'(g)A = A\pi(g)$$

for all $g \in G$

Such a matrix $A \in \mathbb{C}^{n \times m}$ is an intertwining operator (a linear transformation which respects/preserves the action of G).

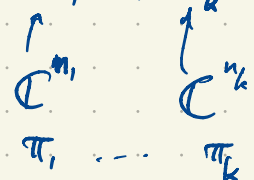
i.e. $\alpha A = A \alpha$ for all $\alpha \in \mathbb{C}G$.

$\alpha(Av) = A(\alpha v)$ A is a homomorphism of $\mathbb{C}G$ -modules.

If $V = \mathbb{C}^m$ and $W = \mathbb{C}^n$ are irreducible (simple) $\mathbb{C}G$ -modules (π, π' irred. representations):

- (i) inequivalent $\Rightarrow A = 0$
- (ii) $\pi \cong \pi'$ equivalent $\Rightarrow A = \lambda \cdot$ fixed invertible $n \times m$ matrix.

p.10 of handout. Theorem 4.4 (Wedderburn's Theorem)
 Let $R = \mathbb{C}G$, $|G| < \infty$. Let M_1, \dots, M_k be the distinct R -modules up to isomorphism.



The M_i -homogeneous part of R is the sum of all the left ideals of R isomorphic to M_i .

eg. $R = M(3, \mathbb{C})$. has only one simple module up to isomorphism, \mathbb{C}^3 .

$A \in R$ acts on $V = \mathbb{C}^3$ by $v \mapsto Av$.

$$R = \begin{bmatrix} * & 0 & 0 \\ * & 0 & 0 \\ * & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & * & 0 \\ 0 & * & 0 \\ 0 & * & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix} \quad \text{contains } \begin{bmatrix} a & b & 0 \\ b & b & 0 \\ c & c & 0 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

Minimal Simple

Submodules (left ideals) of the regular representation are all isomorphic to \mathbb{C}^3 as R -modules.

The \mathbb{C}^3 -homogeneous part of this module is all of R .

$$R = \left[\begin{array}{c|c} \boxed{1*} & 0 \\ \hline * & * \\ * & * \\ \hline 0 & \boxed{***} \end{array} \right] \quad \text{Semisimple of dimension 4.}$$

$$\begin{aligned} \dim M_i &= n_i \\ \dim M_i(R) &= n_i^2 \end{aligned}$$

R has three iso. types of simple modules of dimension 1, 2, 3.

$$R = \begin{bmatrix} * & 0 & 0 \\ 0 & \boxed{0} & 0 \\ 0 & 0 & \boxed{0} \end{bmatrix} \oplus \begin{bmatrix} 0 & * & 0 \\ * & * & 0 \\ 0 & * & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & * \\ * & * & * \\ * & * & * \end{bmatrix}$$

$M_1(R) \qquad M_2(R) \qquad M_3(R)$

If $n_i = \dim M_i$
 then the M_i -homo. part of $R = \mathbb{C}G$ is the sum of all submodules isomorphic to M_i .

R semisimple algebra over \mathbb{C}

$\text{End}_R(R) = \{ \underbrace{R\text{-endomorphisms of } R}_{\text{into itself}} \}$ is the set of maps $\phi: R \rightarrow R$ such that $\phi(rx) = r\phi(x)$ for all $r, x \in R$

Lemma $\text{End}_R(R)$ is anti-isomorphic to R .

For every $a \in R$ we have $\phi_a: R \rightarrow R$, $\phi_a(x) = xa$.

$$\phi_a(rx) = rxa = r\phi_a(x) \Rightarrow \phi_a \in \text{End}_R(R).$$

The map $R \rightarrow \text{End}_R(R)$, $a \mapsto \phi_a \in \text{End}_R(R)$ is bijective.

If $a \in R$ such that $\phi_a = 0$ then $\phi_a(1) = 0$ so $a = 0$. So $a \mapsto \phi_a$ is one-to-one.

$$\phi_{ab}(r) = rab = \phi_b(ra) = \phi_b(\phi_a(r)) = \phi_b \circ \phi_a(r) \Rightarrow \phi_b \circ \phi_a = \phi_{ab}$$

If G is a group then $a \mapsto a^{-1}$ is an anti-automorphism $f(ab) = f(b)f(a)$
Similarly with an algebra.

If R is an algebra then the opposite algebra R° is the algebra with the same elements as R with same vector space structure; only the multiplication is replaced by $x * y = \underbrace{yx}_{\text{in } R}$ $x(yz) = x * (y * z) = (zy)x = z(yx) = (x * y) * z$

R° is not necessarily isomorphic to R . It is anti-isomorphic.

$G^\circ \cong G$ because we can compose two anti-isomorphisms to get an isomorphism
 $G \xrightarrow{\text{inverse}} G \rightarrow G^\circ$ If R is a division algebra then $R^\circ \cong R$ in the same way.

What are the R -endomorphisms of $R = \mathbb{C}G$? $\text{End}_R(R) = R^o$.

$R = I_1 \oplus I_2 \oplus \dots \oplus I_m$ as a direct sum of minimal left ideals.

If $\phi \in \text{End}_R(R)$ then we can represent ϕ using an $m \times m$ matrix over R :

$$\phi(r) =$$

$$r = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \quad r_i \in I_i$$

$r = r_1 + \dots + r_m$ unique choice of $r_i \in I_i$

$\phi(r) = \phi(r_1) + \dots + \phi(r_m)$, decompose each term with respect to our decomposition

$$= \sum_{i=1}^m \left(\sum_{j=1}^m \phi_{ij} \cdot (r_j) \right)$$

$$\phi_{ij} \in \text{Hom}_R(I_j, I_i) = \begin{cases} 0 & \text{if } I_i \not\cong I_j \\ \mathbb{C}I_{n_i} & \text{if } I_i \cong I_j \end{cases}$$

Schur's Lemma

ϕ is represented by $m \times m$ matrix over \mathbb{C}

$$\begin{bmatrix} \phi_{11} & \phi_{12} & \dots & \phi_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{m1} & \dots & \dots & \phi_{mm} \end{bmatrix} = \begin{bmatrix} \begin{matrix} * & \dots & * \\ * & \dots & * \\ * & \dots & * \end{matrix} & \dots & \begin{matrix} * & \dots & * \\ * & \dots & * \\ * & \dots & * \end{matrix} & \dots & \begin{matrix} * & \dots & * \\ * & \dots & * \\ * & \dots & * \end{matrix} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

$\in M(n_1, \mathbb{C})$ \uparrow $M(n_2, \mathbb{C})$

$\text{End}_R(R)$ anti-iso. to $\bigoplus_{i=1}^k M(n_i, \mathbb{C})$

\parallel
 R^o anti-iso
 $= R$

$R = \mathbb{C}G$ has an anti-isomorphism $\sum a_g g \mapsto \sum a_g g^{-1}$

$$R \cong \bigoplus_{i=1}^k M(n_i, \mathbb{C})$$

p. 29 The center of the group algebra

G finite group $n = |G| = \dim \mathbb{C}G$

$$Z(\mathbb{C}G) = \{ \alpha \in \mathbb{C}G : \alpha \gamma = \gamma \alpha \text{ for all } \gamma \in \mathbb{C}G \} \subseteq \mathbb{C}G \text{ subalgebra}$$

$\dim Z(\mathbb{C}G) = k = \text{number of conjugacy classes of } G$

K_1, K_2, \dots, K_k : conjugacy classes of $G = K_1 \sqcup \dots \sqcup K_k$ partition

$$K_1 = \{1\}$$

$$\sum_{i=1}^k |K_i| = n = |G|$$

$$\text{Irr}(G) = \{ \chi_1, \chi_2, \dots, \chi_k \} \quad n_i = \chi_i(1) = \deg \chi_i$$

$$n_1^2 + n_2^2 + \dots + n_k^2 = n$$

Moreover $n_i | n$ which we will prove today or Monday.

Irr. reps. of G are $\pi_j: G \rightarrow \text{GL}_{n_j}(\mathbb{C})$

Basis for $Z(\mathbb{C}G)$ is $\{ \gamma_1, \gamma_2, \dots, \gamma_k \}$ where $\gamma_i = \text{sum of elements in } K_i$. Reps of K_1, \dots, K_k are $\gamma_1, \dots, \gamma_k$

$$\mathbb{C}G \cong \bigoplus_{i=1}^k M(n_i, \mathbb{C}) = \left[\begin{array}{ccc} \begin{array}{c} n_1 \times n_1 \\ * \\ \end{array} & \dots & \begin{array}{c} n_k \times n_k \\ * \\ \end{array} \\ \begin{array}{c} n_2 \times n_2 \\ \end{array} & \dots & \begin{array}{c} n_k \times n_k \\ \end{array} \end{array} \right]$$

$$Z(\mathbb{C}G) \cong Z\left(\bigoplus M(n_i, \mathbb{C})\right) = \left\{ \left[\begin{array}{ccc} \omega_1 I_{n_1} & & \\ & \omega_2 I_{n_2} & \\ & & \ddots \\ & & & \omega_k I_{n_k} \end{array} \right] : \omega_1, \dots, \omega_k \in \mathbb{C} \right\}$$

The iso. $\mathbb{C}G \rightarrow \bigoplus_{i=1}^k M(n_i, \mathbb{C})$ is defined on our basis $g \mapsto \left[\begin{array}{ccc} \pi_1(g) & & \\ & \pi_2(g) & \\ & & \ddots \\ & & & \pi_k(g) \end{array} \right]$

$\pi_j: G \rightarrow GL_{n_j}(\mathbb{C})$ is a group homo. extending to algebra homo.

$\pi_j: \mathbb{C}G \rightarrow M(n_j, \mathbb{C})$, defined by $\pi_j(\sum_g a_g g) = \sum_g a_g \pi_j(g)$.

Restrict to $z \in Z(\mathbb{C}G)$. $zg = gz$ for all $g \in G$

$$\Rightarrow \pi_j(z) \pi_j(g) = \pi_j(zg) = \pi_j(gz) = \pi_j(g) \pi_j(z) \Rightarrow \pi_j(z) = c I_{n_j}, \text{ since } c \in \mathbb{C}$$

In particular $\pi_j(\gamma_i) = \underbrace{\omega_j(\gamma_i)}_{\in \mathbb{C}} I_{n_j}$ since $\gamma_i \in Z(\mathbb{C}G)$ by Schur's lemma.

Denote $\omega(\gamma_i) = \omega_j(\gamma_i) = \omega_\chi(\gamma_i)$ where $\chi = \chi_j = \text{tr } \pi_j$.

$\pi_j(\gamma_i) = \omega_j(\gamma_i) I_{n_j}$ Take trace on both sides. $\gamma_i = \sum_{g \in K_i} g$

$$|K_i| \text{tr } \pi_j(g_i) = |K_i| \chi_j(g_i) = n_j \omega_j(\gamma_i) = \chi_j(1) \omega_j(\gamma_i)$$

$$\omega_\chi(\gamma_i) = \frac{|K_i| \chi(g_i)}{\chi(1)}$$

(p. 30)

We will see that these values $\omega_\chi(\gamma_i)$ are algebraic integers.

pos. integers

algebraic integers
i.e. root of ^{monic} poly.
with coeffs in \mathbb{Z} .

integers with

To show $\frac{n}{n_i} \in \mathbb{Z}$, show it's an algebraic integer and a rational number.

Use $\{\text{alg. integers}\} \cap \mathbb{Q} = \mathbb{Z}$

$Z(\mathbb{C}G)$ is an algebra. (subalgebra)

In particular $\gamma_i \gamma_j \in Z(\mathbb{C}G) \Rightarrow \gamma_i \gamma_j = \sum_{l=1}^k a_{ijl} \gamma_l$

$a_{ijk} \in \mathbb{Z}$

a_{ijl} ($i, j, l \in \{1, 2, \dots, k\}$) are the structure constants of $Z(\mathbb{C}G)$.

Additively, $Z(\mathbb{C}G) \cong \mathbb{C}^k$
 $\sum_{j=1}^k b_j \gamma_j$

$Z(\mathbb{Z}G) =$ algebra gen. by $\gamma_1, \dots, \gamma_k$ over \mathbb{Z}
 $\{ \sum_j b_j \gamma_j : b_j \in \mathbb{Z} \}$

Additively: \mathbb{Z}^k

The multiplicative structure is entirely described by the struct. constants a_{ijl} .

a_{ijl} = ~~brunk~~ determined using the char. table of G .

Eg. $G = S_3 = \underbrace{\{()\}}_{K_1} \sqcup \underbrace{\{(12), (13), (23)\}}_{K_2} \sqcup \underbrace{\{(123), (132)\}}_{K_3}$

In $\mathbb{Z}G \subset \mathbb{C}G$

$\gamma_1 = ()$, $\gamma_2 = (12) + (13) + (23)$, $\gamma_3 = (123) + (132)$

$\gamma_1 \gamma_2 = \gamma_2$, $\gamma_1 \gamma_3 = \gamma_3$, $\gamma_1 \gamma_1 = \gamma_1$

$\gamma_2 \gamma_2 = ((12) + (13) + (23))((12) + (13) + (23)) = 3() + 3(123) + 3(132) = 3\gamma_1 + 3\gamma_3$

$\gamma_3 \gamma_3 = ((123) + (132))((123) + (132)) = 2() + (123) + (132) = 2\gamma_1 + \gamma_3$

$\gamma_2 \gamma_3 = \gamma_3 \gamma_2 = ((12) + (13) + (23))((123) + (132)) = 2\gamma_2$

In a large group, these expansions look unmanageable this way but: we can compute a_{ijk} directly from the character table of G .

In S_3 , each 3-cycle can be expressed as a product of two transpositions in exactly $a_{223} = 3$ different ways.

$\pi(z) = \omega_\chi(z) I$ for all $z \in Z(CG)$, where $\pi: G \rightarrow GL_n(\mathbb{C})$ irred. rep. with character χ
 $\omega_\chi(\gamma_i) = \frac{|K_i| \chi(\gamma_i)}{\chi(1)}$ $\omega_\chi: Z(CG) \rightarrow \mathbb{C}$ is an algebra homo; $\omega_\chi(zz') = \omega_\chi(z)\omega_\chi(z')$ for all $z, z' \in Z(CG)$.

Theorem The structure constants of $Z(CG)$ are $a_{ijl} = \frac{|K_i| |K_j|}{|G|} \sum_{\chi \in \text{Irr}G} \frac{\chi(\gamma_i) \chi(\gamma_j) \overline{\chi(\gamma_l)}}{\chi(1)}$ (non-negative integers)

Proof $\gamma_i \gamma_j = \sum_{l=1}^k a_{ijl} \gamma_l$ $\omega_\chi(\gamma_i) = \frac{|K_i| \chi(\gamma_i)}{\chi(1)}$ Apply this homomorphism to $Z(CG)$ on both sides:

$\frac{|K_i| \chi(\gamma_i)}{\chi(1)} \cdot \frac{|K_j| \chi(\gamma_j)}{\chi(1)} = \sum_{l=1}^k a_{ijl} \frac{|K_l| \chi(\gamma_l)}{\chi(1)}$ Now multiply both sides by $\chi(\gamma_s) \overline{\chi(\gamma_s)}$ ($s=1, 2, \dots, k$) to get

$$\begin{aligned} \sum_{\chi} \frac{|K_i| |K_j| \chi(\gamma_i) \chi(\gamma_j) \overline{\chi(\gamma_s)}}{\chi(1)} &= \sum_{\chi} \sum_{l=1}^k a_{ijl} |K_l| \chi(\gamma_l) \overline{\chi(\gamma_s)} \\ &= \sum_{l=1}^k a_{ijl} |K_l| \underbrace{\sum_{\chi} \chi(\gamma_l) \overline{\chi(\gamma_s)}}_{\delta_{ls} \frac{|G|}{|K_l|}} \\ &= |G| a_{ijs} \quad \square \end{aligned}$$

Sum over $\chi \in \text{Irr}(G)$ and use col. orthogonality of char table of G

$$\begin{aligned} \sum_{\chi \in \text{Irr}G} \chi(\gamma_l) \overline{\chi(\gamma_s)} &= \begin{cases} 0, & \text{if } l \neq s \\ |C_G(\gamma_l)|, & \text{if } l = s \end{cases} \\ &= \frac{|G|}{|K_l|} \end{aligned}$$

So why are $\omega_\chi(\gamma_i) \in \mathbb{Z}$?

$$\gamma_i \gamma_j = \sum_{\ell=1}^k a_{ij\ell} \gamma_\ell$$

$$\omega_\chi(\gamma_i) \omega_\chi(\gamma_j) = \sum_{\ell=1}^k a_{ij\ell} \omega_\chi(\gamma_\ell)$$

In $Z(CG)$, we consider left-multiplication by $\omega_\chi(\gamma_i)$ as a linear transformation with $k \times k$ matrix

$$A_i = A = [a_{ij\ell}]_{j,\ell=1,\dots,k}$$

(fixed:)
 $\det(tI_k - A)$ is a monic poly. with integer coeffs.
 $\Rightarrow \omega_\chi(\gamma_i)$ is an alg. integer

If $v = \begin{bmatrix} \omega_\chi(\gamma_1) \\ \vdots \\ \omega_\chi(\gamma_k) \end{bmatrix}$ then $Av = \omega_\chi(\gamma_i)v$ so v is an eigenvector with eigenvalue $\omega_\chi(\gamma_i)$.

Check $v \neq 0$: on Wednesday. First entry $\omega_\chi(\gamma_i) = |K_i| \omega_\chi(g_i)$

Column orthogonality of char. table of G : $g_i = 1, |K_i| = 1$
 $\pi(r) = \pi(g) = \omega_\chi(r) I_{n_j}$
 $\deg \pi = \deg \chi = \chi(1)$

$$\sum_{\chi \in \text{Irr } G} \chi(g_i) \overline{\chi(g_j)} = |C_G(g_i)| \delta_{ij}$$

$$\text{For } i=j: \sum_{\chi \in \text{Irr } G} \chi(g_i) \overline{\chi(g_i)} = |C_G(g_i)| = \frac{|G|}{|K_i|}$$

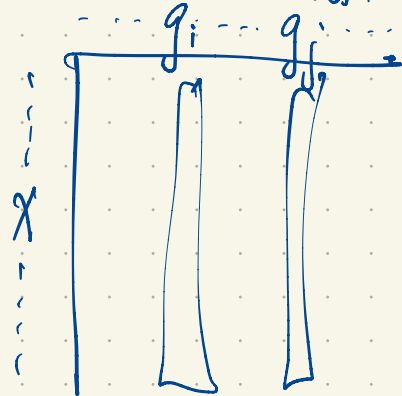
$$|G| = \sum_{\chi} |K_i| \chi(g_i) \overline{\chi(g_i)}$$

$$|K_i| = [G : C_G(g_i)]$$

$$\omega_\chi(\gamma_i) = \frac{|K_i| \chi(g_i)}{\chi(1)}$$

$$\chi(1) \omega_\chi(\gamma_i) = |K_i| \chi(g_i)$$

$\chi(1)$ is an alg. int. $\omega_\chi(\gamma_i)$ is an alg. int.



$$\frac{|G|}{|\chi(1)|} = \sum_{\chi} [\text{alg. int.}]$$

is an alg. int. Also in \mathbb{Q} .
 $\Rightarrow \frac{|G|}{\chi(1)} \in \mathbb{Z}$

$$\Rightarrow \chi(1) \mid |G|$$

The order of every irred. rep. of G divides $|G|$.

$$\omega_\chi(\gamma_i) \in \mathbb{Z}$$

Burnside's Theorem Every group of order $p^a q^b$ (p, q prime; $a, b \geq 0$ integers) is solvable.

There are no nonabelian simple groups of order $p^a q^b$.

The proof (see notes) requires char. theory.

In a finite group G , a difference set is a subset $D \subset G$ such that every nonidentity element $g \in G$ can be expressed as $g = d_1 d_2^{-1}$ ($d_1, d_2 \in D$) in exactly r ways.

Eg. $G = \{1, g, \dots, g^6\}$

$$D = \{g, g^2, g^4\}$$

cyclic of order 7.

$$\begin{aligned} g^2 g^{-1} &= g \\ g^4 (g^2)^{-1} &= g^2 \\ g^4 g^{-1} &= g^3 \\ g (g^4)^{-1} &= g^4 \\ g^2 (g^4)^{-1} &= g^5 \\ g (g^2)^{-1} &= g^6 \end{aligned}$$

In $\mathbb{Z}/7\mathbb{Z}$, $D = \{1, 2, 4\}$

$$\begin{aligned} 2-1 &= 1 \\ 4-2 &= 2 \\ 4-1 &= 3 \\ 1-4 &= 4 \\ 2-4 &= 5 \\ 1-2 &= 6 \end{aligned}$$

$(7, 3, 1)$ -diff set in C_7 .

If $|G| = v$ and $|D| = k$ then $k(k-1) = r(v-1)$. D is a (v, k, r) -diff. set in G .

$$\begin{aligned} 3 \cdot 2 &= 1 \cdot (7-1) \\ 6 &= 6 \end{aligned}$$

When does a (v, k, r) -diff. set exist in a group of order v ?

Techniques work best when G is abelian. But there are nontrivial diff. sets in some nonabelian groups. Eg. $G =$ Frob. gp. of order 21 (the nonabel. gp. of order 21) has a nontriv.

$(21, 5, 1)$ -diff. set.

$$\begin{aligned} 5 \cdot (5-1) &= 1 \cdot (21-1) \\ 20 &= 20 \end{aligned}$$

Also a diff. set in the cyclic gp. of order 21.

Both examples arise from the proj. plane of order 21.

If D is a (v, k, r) -diff. set in a gp G then v subsets of size k in a set of size v

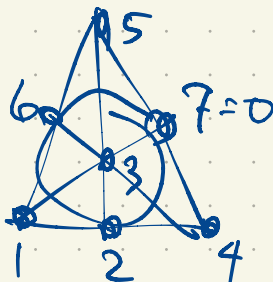
Any two of them intersect in r points
any two pts are in exactly r blocks.

$\{D_g : g \in G\}$ form a (v, k, r) -design:
(the v blocks of the design) symmetric

$$D = \{1, 2, 4\} \text{ in } G$$

$$D+1 = \{2, 3, 5\}$$

$$D+2 = \{3, 4, 6\}$$



The fact that $D \subset G$ is a (v, k, r) -diff. set can be expressed succinctly in the group ring $\mathbb{Z}G$:

$$Y = \sum_{g \in G} g, \quad S = \sum_{d \in D} d$$

$\mathbb{Z}G$ has an involutory anti-automorphism $\alpha \mapsto \alpha^*$

If $\alpha = \sum_{g \in G} a_g g$ then $\alpha^* = \sum_{g \in G} a_g g^{-1}$

$(\alpha^*)^* = \alpha$
 $(\alpha\beta)^* = \beta^* \alpha^*$

$$SS^* = n + rY \text{ where } n = k - r \quad n = \text{order of the design (or the difference set)}$$

$$= k + r(Y-1) = \underbrace{(k-r)}_n + rY$$

Ex. $D = \{g, g^2, g^4\}$ in $G = \{1, g, g^2, \dots, g^6\}$ cyclic of order 7

$$S = g + g^2 + g^4$$

$$SS^* = (g + g^2 + g^4)(g^{-1} + g^{-2} + g^{-4}) = 3 + g + g^2 + g^3 + g^4 + g^5 + g^6 = 2 + Y$$

Let $\chi \in \text{Irr } G$. So $\chi(1) = 1$.

$\chi: \mathbb{Z}G \rightarrow \mathbb{C}$ is an algebra homo. (ring)

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

If $\chi = \chi_1 = \text{principal character}$ then $\chi(\sum a_g g) = \sum a_g$ "augmentation map"

$$\chi(S) = k, \quad \chi(Y) = v$$

$$SS^* = n + rY \Rightarrow k^2 = n + rv \Rightarrow n = k - r = k^2 - rv$$

$$rv - r = k^2 - k$$

$$(v-1)r = k(k-1)$$

To prove this without characters, just a double counting argument:
 Count ordered pairs $d_1 \neq d_2$ in D .

$k(k-1) = r(v-1)$
 choices for $d_1 \in D$ choices for $d_2 \in D$

$(7, 3, 1)$ -diff. set of order 2

	1	g	g ²	...	g ⁶
χ_1	1	1	1	...	1
χ_2	1	ζ	ζ^2	...	ζ^6
...	1	ζ^2	ζ^4	...	ζ^5
...	1
χ_7	1	ζ^6	ζ^5	...	ζ

$\zeta = e^{2\pi i/7}$

Now let χ be nonprincipal.

$$|\chi(S)|^2 = n \Rightarrow |\chi(S)| = \sqrt{n}$$

$$\chi(S) \overline{\chi(S)} = n + r\chi(S)$$

$$\chi(\sum a_g g) = \sum a_g \chi(g)$$

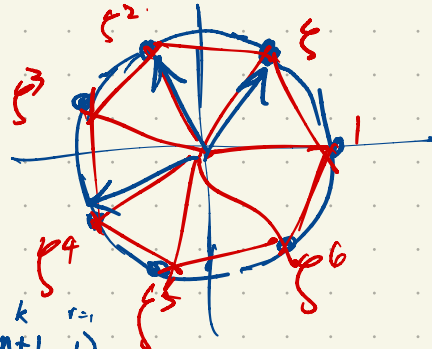
$$\chi((\sum a_g g)^*) = \chi(\sum a_g g^{-1}) = \sum a_g \chi(g^{-1}) = \overline{\sum a_g \chi(g)}$$

eg. $D = \{g, g^2, g^4\}$

$S = g + g^2 + g^4$

$\chi(S) = \xi + \xi^2 + \xi^4$, $\xi = e^{2\pi i/7}$

$|\chi(S)| = \sqrt{7}$



In $G = C_n$, $|D| = n+1$, $D \subset G$ is a ^{$(\frac{n^2+n+1}{2}, \frac{n+1}{2}, 1)$} diff. set iff $|\chi(S)| = \sqrt{n}$ for all nonprincipal characters of C_n .

Given a finite group G with $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, χ_1, \dots, χ_k form a basis for all class functions $G \rightarrow \mathbb{C}$.

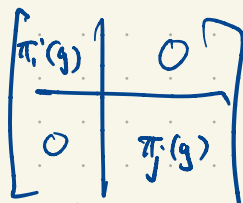
$\chi_i + \chi_j$ is a class function.

$\chi_i \chi_j \dots \Rightarrow \chi_i \chi_j =$ linear comb. of irred. chars of G .

$\chi_i(g) = \text{tr } \pi_i(g)$

$\chi_j(g) = \text{tr } \pi_j(g)$

$(\chi_i + \chi_j)(g) = \text{tr}$



$(\chi_i \chi_j)(g) = \chi_i(g) \chi_j(g) = \text{tr}$

?
 what representation
 has $\chi_i \chi_j$ as its character
 i.e. trace

$\chi_i(1) + \chi_j(1)$
 $\frac{\chi_i(1)}{n_i} \frac{\chi_j(1)}{n_j}$

If A, A' are $m \times m$
 B, B' are $n \times n$

$$(A \otimes B)(A' \otimes B') = (AA') \otimes (BB')$$

then $A \otimes B$ is $mn \times mn$:

$A \otimes B =$

$a_{11}B$	$a_{12}B$...	$a_{1m}B$
$a_{21}B$	$a_{22}B$...	$a_{2m}B$
...
$a_{n1}B$	$a_{n2}B$...	$a_{nm}B$

$\text{tr}(A \otimes B) = (a_{11} + a_{22} + \dots + a_{nn}) \text{tr} B = (\text{tr} A) \text{tr} B$

Character table of S_5 using newer content on representations

$(C_G(g))$	20	12	8	6	4	5	6
g	(1)	(12)	(12)(34)	(123)	(1234)	(12345)	(123)(45)
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	1	-1
χ_3	4	2	0	1	0	-1	-1
χ_4	4	-2	0	1	0	-1	1
χ_5	5						
χ_6	5						
χ_7	6						

χ	5	3	1	2	1	0	0
$\chi_i = \chi - \chi_i$	4	2	0	1	0	-1	-1

$[\chi_i, \chi_i] = 1$. Check!

$$120 = 1^2 + 1^2 + 4^2 + 4^2 + \underbrace{n_5^2 + n_6^2 + n_7^2}_{36}$$

$n_5, n_6, n_7 \in \{2, 3, 4, 5, 6, \cancel{7}\}$
 $n_5^2, n_6^2, n_7^2 \in \{4, 9, 16, 25, 36, \cancel{49}\}$

$n_i \mid |G|$

$$[\chi_1, \chi_1] = \frac{1}{120} + \frac{1}{12} + \frac{1}{8} + \frac{1}{6} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = 1$$

$$[\chi, \chi] = \frac{5^2}{\frac{120}{24}} + \frac{3^2}{\frac{120}{24}} + \frac{1}{8} + \frac{4}{6} + \frac{1}{4} + 0 + 0$$

$$= \frac{5 + 18 + 3 + 16 + 6 + 0 + 0}{24} = \frac{48}{24} = 2$$

$[\chi, \chi_i] = 1$ as before

$\chi = \chi_i + \chi_i, \chi_i \neq \chi_i$

$\chi = \sum a_i \chi_i$

$[\chi, \chi] = \sum a_i^2$

Another way to know χ_i is irreducible: χ is a perm. character of a doubly trans. perm. group. We'll prove this later!