Group Representations MATH 607

Thanic Nur Samin

Texts: Lang, Algebra, Revised Third Edition, Chapter 17 (sections 1-5) and 18 (sections 1-8)
Serre, Linear Representations of Finite Groups, Parts II and III

Monday, 8/26/2024

Today:
History
Modular
Quotients
Matrices
Lang XVII, Section 1

(Fake) History

History of Groups
Most notions (let's say what is a vector spce, what is a group) were vague.
Originally, groups were seen as:

- Symmetry Groups S_n
- $GL_n(\mathbb{R})$ aka $n \times n$ invertible matrices
- Subgroups of the above
- Representations of the above

For representation, consider G and a homomorphism $G \to S_n$ [which is a group action $G \curvearrowright \{1, 2, \dots, n\}$] or a homomorphism $G \to GL_n$ [which is a group action on vector space].
Part I of this course will be Ring Theory.

Part I: Ring Theory

Module

Convention: $R =$ Ring with unity

Definition (Left Module)**.** Left Module is an abelian group M with a function $R \times M \to M$ so that $(r, m) \mapsto rm$ such that $R \times M \to M$ is $\mathbb{Z}$-billinear.
Meaning, we have:
$(r + r')m = rm + r'm$
$r(m + m') = rm + rm'$
Also $(rr')m = r(r'm)$
And finally $1m = m$

By default, module = left module (since Jim doesn't want Trump to get reelected, he prefers left module)
module / field [module over field] = vector space
We can have submodules $M' \triangleleft M$
We have quotients M/M'
We have the short exact sequence:

$$0 \to M' \to M \to M/M' \to 0$$

which means in each homomorphism, im = ker
So, $M' \to M$ is injective and $M \to M/M'$ is surjective.
Also, kernel of $M \to M/M'$ is M'

Remark. Note that R is itself an R-module.
Convention: Submodule M of R = left ideal of R.
Left ideals are not enough to take quotients (like how we need normal subgroup for group quotients).

So we need two sided ideals.

Definition (Two Sided Ideals)**.** $I \subset R$ is <u>2-sided ideal</u> if I is abelian subgroup and $ri \in I, ir \in I$ aka "closed".

Example. Consider a homomoprhism $f : R \to R'$. Then $\ker f$ is a 2-sided ideal of R.

For ring homomorphism we need:
$f(r + r') = f(r) + f(r')$
$f(rr') = f(r)f(r')$
$f(1) = 1$
If $I \subset R$ is 2-sided then R/I is a quotient ring.
For example, $M_2(\mathbb{R})$ has no proper 2-sided ideal. But there exists left ideals!
$\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$ is a left ideal
Matrices are a good 'source' of non-commutative rings.
Given any ring R we can consider ring $M_n(R)$ of $n \times n$ matrices.
Given R-module M we can get $\mathrm{End}_R(M) = \{f : M \to M, f \text{ is } R\text{-module map}\}$
We have $(f + g)m = f(m) + g(m), (fg)m = f(g(m))$.
This is a 'coordinate free approach' to matrices.

Remark. $M_n(R)$ and $\mathrm{End}_R(R^n)$ often looks the same, but in general $M_n(R) \ncong \mathrm{End}_R(R^n)$.

Let's first take $n = 1$. Let $r_0 \in R$.
Consider $R \to R$ map $r \mapsto r_0 r$
We don't like this because <u>this is not a left module map!!!</u>
So this is not even in $\mathrm{End}_R(R)$
What if we consider $r \mapsto r r_0$?
This is a left module map, aka $\in \mathrm{End}_R(R)$
But $R \to \mathrm{End}_R(R)$ is not a ring homomorphism.
So we are going to take the opposite ring.
<u>Fix 1</u>:
Given ring R, we can look into the mirror and find opposite ring R^{op}
Elements of R^{op} = elements of R.
$0, 1, +$ remain the same
But multiplication is reversed: define $r \cdot_{op} r' = r'r$
Alternate notation, we write *op* on elements.
Then $r^{op}(r')^{op} = (r'r)^{op}$
Then we have isomorphism $R^{op} \cong \mathrm{End}_R(R)$ which is a ring homomoprhism!

Exercise.

1) $R \cong R^{op} \iff \exists$ antiautomorphism $\alpha : R \to R$

   Antiautomorphism means α preserves $0, 1, +$ but reverses mutliplication

2) R commutative, then $(M_n R) \cong (M_n R)^{op}$

3) Real quaternions $\mathbb{H} \cong \mathbb{H}^{op}$

Remark. If you take right modules, you don't need op.

There is a <u>contravariant endofunctor</u> in the category of rings which takes objects of rings to their opposite.
$\text{Ring}^{op} \to \text{Ring}$ [opposite category, not the same thing]
$R \mapsto R^{op}$
<u>Fix 2</u>: [From Lang]
Suppose we have module homomorphism $\phi : E = E_1 \oplus \cdots \oplus E_n \to F_1 \oplus \cdots \oplus F_m = F$
Then we have $E_j \to E \xrightarrow{\phi} F \to F_i$ which we define to be $E_j \xrightarrow{\phi_{ij}} F_i$
Then we have a matrix $M(\phi)$ so that $M(\phi) = (\phi)_{ij}$
Then for $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in E_1 \oplus \cdots \oplus E_n$
Then $\phi(x) = (\phi_{ij}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
So, if we have $E^n = E \oplus \cdots \oplus E$ [n times]
Lang says, there is a ring isomorphism

$$\text{End}_R(E^n) \xrightarrow{\cong} M_n(\text{End}_R E)$$

$$\phi \mapsto (\phi_{ij})$$

If $E = R$ as left module, then $\text{End}_R R \cong R^{op}$
By combining these, $\text{End}_R(R^n) \cong M_n(R^{op})$

Wednesday, 8/28/2024

Today:
Group ring
Category
Simple modules
Question: The course is about 'group representations'. So why study rings?
Answer: A group representation [homomorphism $G \to GL_n(\mathbb{R})$] is exactly the same as a module over the ring $\mathbb{R}G$.
So knowing everything about modules would tell us everything about representation.
Abelian Category!
Suppose we have a ring R and a group G. We can get a ring out of G

Definition (Group Ring RG)**.** As an abelian group, this is the free R-module with basis the elements of G.
Elements are symbols of the form $r_1g_1 + \cdots + r_ng_n$ [finite linear combination].
0 is the trivial linear combination. So $0 = 0$
$1 = 1e = 1_R e_G$
Multiplication is defined in the obvious way.
$(\sum_i r_i g_i)(\sum_j r'_j g'_j) = \sum_{i,j} r_i r'_j g_i g'_j$

Suppose V is a R-module.
Then a homomorphism $\rho : G \to \text{Aut}_R(V) \leftrightarrow V$ is RG-module.
$\rho \mapsto (\sum_i r_i g_i)v := \sum_i r_i \rho(g_i)v$
$g \mapsto (v \to gv) \leftarrow V$ RG module.

Example. $C_2 = \{1, t\}$
Then we have $\mathbb{Z}C_2 = \{a + bt \mid a, b \in \mathbb{Z}, t^2 = 0\} = \mathbb{Z}[t]/(t^2)$
Note that $(1+t)(1-t) = 1 - t^2 = 0$ so we have zero divisors.
Take $C_\infty = \langle t \rangle$
Then $\mathbb{Z}C_\infty = \mathbb{Z}[t, t^{-1}]$ the laurent polynomial ring.
$\mathbb{Q}C_\infty = \mathbb{Q}[t, t^{-1}]$ is a PID [since it is a euclidean ring]

Now we see categories.
If we fix R then we have a functor Group $\to$ Ring given by $G \mapsto RG$
Or we could say we have a functor Ring $\times$ Group $\to$ Ring given by $(R, G) \to RG$

Definition. A category $\mathcal{C}$ consists of:

- objects Ob $\mathcal{C}$
- morphism $C(X, Y)$ for $X, Y \in$ Ob $\mathcal{C}$
- compositions $C(X, Y) \times C(Y, Z) \to C(X, Z)$ given by $(g, f) \mapsto f \circ g$
- identity $\mathrm{Id}_X \in C(X, X) \forall X \in \mathrm{Ob}\mathcal{C}$

Such that we have:

- associativity: $(f \circ g) \circ h = f \circ (g \circ h)$
- composition with identity: $\mathrm{Id}_Y \circ f = f = f \circ \mathrm{Id}_X$ for $f \in C(X, Y)$

For example in the cateogry of groups, we have objects groups and morphisms homomorphism.
Morphism notations: $f : X \to Y$ or $X \xrightarrow{f} Y$ for $f \in C(X, Y)$

Definition. $f : X \to Y$ is isomorphism if $\exists g : Y \to X$ such that $f \circ g = \mathrm{Id}, g \circ f = \mathrm{Id}$.
Thehen we say X and Y are isomorphic and write $X \cong Y$.

Example. Example of Categories:

- Set
- Ring
- Group
- Ab (Abelian Groups)
- R-modules (objects are modules, morphisms are homomorphisms $h(rm) = rh(m)$)
- Given a group G we can get a category BG such that:

  Ob $BG = \{*\}$ and $BG(*, *) = G$

  In this category, there is only one object $*$. The elements of the group are morphisms.

Definition. Functor $F : \mathcal{C} \to \mathcal{D}$ is $F :$ Ob $\mathcal{C} \to$ Ob $\mathcal{D}$ given by $X \mapsto F(X)$
And $F : \mathcal{C}(X, Y) \to \mathcal{D}(F(X), F(Y))$ such that
$X \xrightarrow{f} Y$ gives us $F(X) \xrightarrow{F(f)} F(Y)$
such that $F(f \circ g) = F(f) \circ F(g)$ and $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$

Example. Unit Functor Ring $\to$ Group given by $R \mapsto R^\times = \{r \in R \mid \exists s \in R, rs = 1 = sr\}$
For example, $\mathbb{Q}^\times \cong C_2 \oplus \mathbb{Z}^\infty [= \pm p_1^{e_1} p_2^{e_2} \cdots]$
$\mathbb{Z}^\times \cong \{\pm 1\} = C_2$
$(\mathbb{Z}C_2)^\times \cong \{\pm 1, \pm t\} \cong C_2 \times C_2$

Definition. R is a division ring (= skew field) if $1 \neq 0$ and $R^\times = R - 0$.

Definition. Quaternions
$\mathbb{H} = \{a + bi + cj + dh \mid a, b, c, d, \in \mathbb{R}\}$
Where $i^2 = j^2 = k^2 = -1$
$ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$
This is a division ring since we can write down inverses.
$\alpha = a + bi + cj + dk$ gives us $\overline{\alpha} = a - bi - cj - dk$
So, $\mathrm{norm}(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$
So, $\alpha^{-1} = \frac{\overline{\alpha}}{\mathrm{norm}(\alpha)}$

Remark. Note that the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a subgroup of $\mathbb{H}^\times = GL_1(\mathbb{H})$.
So, $\mathbb{H}$ is a $\mathbb{R}Q_8$ module.

Theorem 1 (Weddenburn's Little Theorem)**.** a. A finite commutative domain is a field [easy]
b. A finite skew field is a field [aka commutative]

a is easy: suppose F is finite commutative domain. For $0 \neq f \in F$, consider multiplication by f as a map $F \to F$. It is injective, and finiteness implies surjective. So, it is bijective, and there exsits inverse.
eg $\mathbb{Z}/p$ is a field.

Simple Modules

These are like primes. We also have some analogue of prime factorization.

Definition. R-module E is simple if:
$E \neq 0$
No proper submodules, aka $M \triangleleft E \implies M = 0$ or E
In other words, E is a simple module if it only has two submodules: 0 and E.

eg simple $\mathbb{R}$-modules are 1 dim vector spaces, aka $\mathbb{R}$

Exercise. a) $\mathbb{R}^2$ is a simple $M_2(\mathbb{R})$-module

b) Express $M_2(\mathbb{R})$ as direct sum of simple modules.

Friday, 8/30/2024

Exercise. Suppose finite $G \neq 1$ and $R \neq 0$ Prove that RG has zero divisors.

Definition. Direct product of rings $R \times S$, addition and multiplication is done componentwise.
It is a product in the category of rings. aka:

$$\begin{tikzcd}
 & T \arrow[dl, "f_1"'] \arrow[d, dotted, "f"] \arrow[dr, "f_2"] & \\
R & R \times S \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & S
\end{tikzcd}$$

for any pair of ring homomorphisms $T \xrightarrow{f_1} R$ and $T \xrightarrow{f_2} S$ we have a unique ring homomorphism $f : T \xrightarrow{f} R \times S$ so that the diagram commutes.

Definition. $e \in R$ is an idempotent if $e^2 = e$.

$0, 1$ are trivial idempotents.
$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is an idempotent in $M_2(\mathbb{R})$
$(0, 1)$ is an idempotent in $\mathbb{R} \times \mathbb{R}$
If e is an idempotent so is $1 - e$

Definition. Idempotent $e \in R$ is central if $\forall r$ we have $er = re$

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is not central, but $(0, 1)$ is.

Exercise. A ring can be written as a product ring, aka $R \cong R_1 \times R_2$ with $R_i \neq 0$ if and only if there exists a nontrivial central idempotent.

Semisimiple Modules

Definition. E is a simple R-module if it doesn't have any nontrivial submodules.
If $E \neq 0$ and $M \triangleleft E$ then $M \neq 0$ or $M = E$

Example. R^2 is a simple $M_2\mathbb{R}$-module.
$\mathbb{R} \times 0$ is a simple $\mathbb{R} \times \mathbb{R}$ module.
$\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module

Lemma 2. [Schur's Lemma]: Let E, F be simple R-modules. Then any nonzero homomoprhism $f : E \to F$ is an isomorphism.

Proof. $f \neq 0$ means $\ker f \neq E$ and $\operatorname{im} f \neq 0$.
Since they are submodules, $\ker f = 0$ and $\operatorname{im} f = F$
So f is bijective. □

Corollary 3. If E is simple, then $\mathrm{End}_R E$ is a skew field [any non-zero element is invertible]

Example. Commutative example: $\mathrm{End}_{M_2\mathbb{R}}(\mathbb{R}^2)$ is a skew field.
In fact, $\mathrm{End}_{M_2\mathbb{R}}(\mathbb{R}^2) \cong \mathbb{R}$

Definition (Direct Sum)**.** Suppose $M_i \triangleleft M$ for $i \in I$
Then, $M = \bigoplus_{i \in I} M_i$ means, $\forall m \in M_i$ we have $m = \sum_{i \in I} m_i$ with $m_i \in M_i$ uniquely.
There are notions of internal and external direct sums. The above is an internal direct sum.
External direct sum: given $\{M_i\}_{i \in I}$ we can construct $\bigoplus_{i \in I} M_i$

Proposition 4 (Universal Property)**.** Given a collection of homomorphisms $\{t_i : M_i \to N\}_{i \in I}$, it extends directly to a homomorphism $\bigoplus M_i \to N$. We denote this by $\bigoplus f_i$

Remark. Note: Maps to product are easy, maps from direct sum are easy.

Proposition 5 (1.2, Lang XVII)**.** Suppose we have isomorphism $E_1^{n_1} \oplus \cdots \oplus E_r^{n_r} \xrightarrow{\cong} F_1^{m_1} \oplus \cdots \oplus F_s^{m_s}$ with E_i and F_j simple and non-isomorphic [ie for all $k \neq i, E_k \ncong E_i$ and $k \neq j, F_k \ncong F_j$]
Then $r = s$ and there exists a permutatation $\sigma \in S_r$ so that $E_j \cong F_{\sigma(j)}$ and $n_j = m_{\sigma(j)}$

Corollary: If E is a finite direct sum of simple modules, then the isomorphism class of simple components of E and multiplicities are well-defined.

Proof. We use Schur's Lemma.
We write ϕ as a matrix $(\phi_{ji} : E_i^{n_i} \to F_j^{m_j})$
Since ϕ is injective, for all i there exists a j such that $\phi_{ji} \neq 0$
Then, $E_i \cong F_j$ by Schur's Lemma
Note that F_j are isomorphic. So, for all i, the j such that $\phi_{ji} \neq 0$ is unique!
We also get $\sigma : \{1, \ldots, r\} \to \{1, \ldots, s\}$ so that $\sigma(i) = j$
Since σ^{-1} exists σ^{-1} exists, and thus $r = s$
Since ϕ is an isomorphism, individual $\phi_{ji} : E_i^{n_i} \to F_{\sigma(i)}^{m_{\sigma(i)}}$ are isomorphisms.
To complete the proof, we need a lemma
Lemma: Let E be simple. If $E^n \cong E^m$ then $n = m$
Proof of lemma; Let $D = \mathrm{End}_R E$. By Schur's Lemma, D is a division ring.
Since $E^n \cong E^m$, we have $\mathrm{End}_R(E^n) \cong \mathrm{End}_R(E^m)$
So, $M_n(D) \cong M_m(D)$
Also, isomorphism not just as rings, but also as D-modules.
Every module over a skew field is free, and the number of dimensions is the same.
So, $n^2 = m^2 \implies n = m$
This finishes the proof.
□

Lang XVII section 2

Theorem 6. Let E be an R-module. Then TFAE:
SS1: E is a sum of simple modules [so, we can write $m \in E$ as sum of m_i but it is not unique]
SS2: E is a direct sum of simple modules [we can write as a sum, and it's unique]
SS3: Every submodule of E is a summand.
$F \triangleleft E \iff$ we can find F' so that $E = F \oplus F'$
SS3$'$: any monomorphism $F \to E$ 'splits'
SS3$''$ Short exact sequence

$$0 \to F \to E \to H \to 0$$

splits.

This leads us to:

Definition. E is semisimple if it satisfies one of the above.

Davies: SS2 is best
eg: $R = \mathbb{R} \times \mathbb{R}$
$E = \mathbb{R} \times \mathbb{R}$ is semisimple but not simple.
Because: $E = \mathbb{R} \times 0 \oplus 0 \times \mathbb{R}$

Wednesday, 9/4/2024

Recap: Semisimple modules.

Lemma 7. If $E = \sum_{i \in I} E_i$ with E_i simple. Then, $\exists J \subset I$ such that $E = \bigoplus_{j \in J} E_j$

Corollary 8. SS1 $\implies$ SS2

Proof. Let $J \subset I$ be maximal such that $\sum_{j \in J} E_j = \bigoplus_{j \in J} E_j$
This exists by Zorn's lemma.
$\forall i \in I - J$, we have $E_i \cap \bigoplus_{j \in J} E_j \neq \varnothing$ by maximality.
Since E_i is simple, $E_i \subset \bigoplus_{j \in J} E_j$. Therefore, $E = \bigoplus_{j \in J} E_j$.

□

<u>True of False</u>? Every module has a maximal proper submodule.
False!!! Exercise.

Exercise. a) If $M \triangleleft F$ proper and M maximal, then F/M is simple.

b) Find a ring R, module M which does not have proper maximal submodules.

c) If F is a finitely generated R-module, then it is contained in a proper maximal submodule.

Proof of SS2 $\implies$ SS3. Suppose $F \triangleleft E = \bigoplus_{i \in I} E_i$ with E_i simple. Let $J \subset I$ be maximal such that:

$$F + \bigoplus_{j \in J} E_j = F \oplus \bigoplus_{j \in J} E_j$$

Take any $i \in I - J$. Then, $E_i \cap \left[F \oplus \bigoplus_{j \in J} E_j\right] \neq 0$ by maximality of J.
Since E_i is simple, $E_i \subset F \oplus \bigoplus_{j \in J} E_j$.
Therefore, $E = F \oplus \underbrace{\bigoplus_{j \in J} E_j}_{F'}$.
We have found F', which proves SS3.

□

Proof of SS3 $\implies$ SS1.

Lemma 9. $0 \neq F \triangleleft E$ and E satisfies SS3. Then, there exists simple finitely generated $S \triangleleft F$.
Plan: $M \underset{\neq}{\triangleleft} \underset{\text{f.g.}}{F_0} \triangleleft F \triangleleft E$.
Then, choose $0 \neq v \in F$. Let $F_0 = Rv$.

Exercise. M exists. [Zorn's Lemma]

Let $E = \sum_{\text{simple } S \triangleleft E} S$.
Then, by SS3, $E = E_0 \oplus E_0'$.
Lemma and definition of E_0 implies: $E_0' = 0$. So, E is indeed a sum of simple R-modules. We're done!

$\square$

Proposition 10 (2.2)**.** Every quotient module and submodule of a semisimple modules is semisimple.

Proof. Quotients: Suppose $M = E/N$. We have surjective $f : E \to M$ with E semisimple.
SS1 implies $E = \sum_{i \in I} S_i$ with S_i simple.
Then, $M = \sum_{i \in I} f(S_i)$
Schur's lemma implies $f(S_i)$ is either 0 or simple, so M satisfies SS1.
Submodules: Suppose $F \triangleleft E$ with E semisimple. SS3 implies $E = F \oplus F'$. Thus $E \cong E/F'$, so it is semisimple by the quotient result.

$\square$

Preview:

Definition. A ring R is semisimple if and only if all R-modules are semisimple.
Lang defines semisimple differently: A ring R is semisimple if it is semisimple as an R-module.

Theorem 11 (Artin-Weddenburn Theorem)**.** A ring is semisimple if and only if it is isomorphic to a finite product of matrix rings over division algebras:

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

$\mathbb{C}G, \mathbb{R}G$ are semisimple. We also have the result:

Theorem 12 (Maschke's Theorem)**.** The group ring kG is semisimple if G is finite and k is a field of characteristic prime to G.
This also works with $\operatorname{char} k = 0$. It is in fact an if and only if.

So $\mathbb{F}_p G$ is also semisimple given $p \nmid |G|$

Proof. Outline: let $|G| = n$. We will verify SS3.
Let $F \triangleleft E$ be kG modules.
k is a field, so there exists a k-linear projection $\pi : E \to F$ such that $\pi(f) = f$ for $f \in F$ [take a basis of F as a k-vector space, complete it to a basis of E].
Now, define an 'average'.

$$\pi'(e) = \frac{\sum_{g \in G} g\pi(g^{-1}e)}{n}$$

Then, $\pi' : E \to F$ is a kG-linear projection, meaning $\pi'(ge) = g\pi'(e)$.
Then $E = \underset{F}{\operatorname{im} \pi'} \oplus \underset{F'}{\ker \pi'}$

$\square$

Friday, 9/6/2024

Lang XVII, Sectiion 3

"Density Theorem"
Suppose R is a ring and E is a R-module. Then we have maps $R \times E \to E$ by mutliplication on the left.

Definition (Commutant)**.** $R' = R'(E) = \mathrm{End}_R(E)$ is a ring.
$\phi \in R' \iff \phi : E \to E$ such that $\phi(re) = r\phi(e)$. It 'commutes with E'.
Note that E is also an R'-module, with $R' \times E \to E$ given by $(\phi, e) = \phi(e)$.

Definition (Double Commutant)**.** We can iterate on the previous definition.

$$R'' = R'(R'E) = \mathrm{End}_{R'}(E)$$

Therefore,

$$R'' = \mathrm{End}_{R'}(E) = \mathrm{End}_{\mathrm{End}\ R(E)}(E)$$

This means, $f \in R'' \iff f : E \to E, \forall \phi \in R', f \circ \phi = \phi \circ f$. So, things in R'':

<u>commute</u> with things which commute with $r \in R$.

Example. Suppose $R = \mathbb{R}$ and $E = \mathbb{R}^n$. Then,

$$\mathbb{R}' = \mathrm{End}_{\mathbb{R}}(\mathbb{R}^n) = M_n(\mathbb{R})$$

$$\mathbb{R}'' = \underset{rI}{\mathrm{End}_{M_n(\mathbb{R})}(\mathbb{R}^n)} \underset{\leftarrow}{=} \underset{r}{\mathbb{R}}$$

Suppose $V =$ vector space.
$V^* = \mathrm{Hom}(V, \mathbb{R})$
Then we have evaluation map $ev : V \to V^*$ given by $v \mapsto (\phi \mapsto \phi(v))$.
ev is 1-1.
ev is onto iff $\dim V < \infty$.
With inspiration from this, we define,

Definition (Evaluation map)**.** $ev : R \to R''$ given b $r \mapsto (e \mapsto re)$
We define $f_r : E \to E$ given by $f_r = ev(r)$

Proposition 13. a) $f_r \in R''$

b) ev is a ring homomorphism.

Proof. a) $f_r(\phi(e)) = r\phi(e) = \phi(re)\phi(f_r(e))$

b) $ev(r + r') = ev(r) + ev(r'), ev(1) = 1.$
$(ev(r))(ev(r'))e = ev(r)(r'e) = rr'e = ev(rr')e$

□

Lemma 14 (3.1)**.** Suppose E is semisimple over R, $e \in E$ and $f \in R''$
Then $\exists r \in R$ such that $re = f(e)$ [i.e. $f(e) = ev(r)(e)$]

Proof. E is semisimple, and Re is a submodule. Therefore, we can write $E = Re \oplus F$.
Define $\pi : E \to E$ be projection to Re.
Then $\pi \in E' \implies f \circ \phi = \pi \circ f \implies f(e) = f(\pi(e)) = \pi(f(e)) = re$ for some $r \in R$. □

We will prove a stronger version of this lemma called the <u>Jacobson Density Theorem</u>.

Theorem 15 (3.2, Jacobson Density Theorem)**.** Suppose E is semisimple over R
$e_1, \cdots e_n \in E$
$f \in R''$
Then, $\exists r \in R$ such that $re_i = f(e_i) \forall i$.
Therefoe, if E is finitely generated over R', then $R \to R''$ is onto.

Proof. We use a diagonal trick.
Special Case: E is simple.
Idea: Apply the lemma on E with $\underline{e} = (e_1, \cdots, e_n)$ and $f^n : E^n \to E^n$ such that $f(y_1, \cdots, y_n) = (f(y_1), \cdots, f(y_n))$.
We need to check that $f \in R'(R'(E))$ to apply it.
This would imply that $f^n \in R'(M_n R) \underset{E \text{ simple}}{=} R'(R'(E^n))$
Therefore, $\exists r$ such that $r\underline{e} = f^n(\underline{e})$. This finishes the proof.
For E semisimple, key idea is $f^n \in R'(R'(E))$ as above. [Complicated for infinite sums. We avoid.]

$\square$

Application:

Theorem 16 (Burnside's Theorem)**.** Suppose k is an algebraically closed field.
Take subring R such that $k \subset R \subset M_n(k)$
If $k^n (= E)$ is a simple R-module, then prove that:

$$R = M_n(k)$$

Exercise. Suppose D_{2n} is the dihedral group of order $2n$, aka

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$$

Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$
Then we can define a homomorphism $D_{2n} \to GL_2(\mathbb{C})$ given by:

$$r \mapsto \begin{bmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{bmatrix}$$

$$s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

This gives us a ring map $\pi : \mathbb{C}D_{2n} \to M_2\mathbb{C}$
Prove the following:

a) Prove that $\mathbb{C}^2$ is a simple $\mathbb{C}D_{2n}$ module [can be done without technology]

b) Use Burnside's theorem to show that π is onto.

Note that Burnside's theorem doesn't work if k is not algebraically closed.
We have:

$$\mathbb{R} \subset \mathbb{C} \subset M_2\mathbb{R}$$

since we can embed $\mathbb{C}$ into $M_2\mathbb{R}$.
$\mathbb{C}$ is a simple R module, but $\mathbb{C} \neq M_2\mathbb{R}$

Proof of Burnside's Theorem. Step 1: We show that $\mathrm{End}_R(E) = k$
Note that, $k \underset{\text{central}}{<} \underset{\text{skew field}}{\mathrm{End}_R(E)} \subset \underset{\text{finite dim}/k}{\mathrm{End}_k(E)}$
$\forall \alpha \in \mathrm{End}_R(E), k(\alpha)$ is a field and finite dimensional $/k$.
Therefore, $k(\alpha) = k$ since k is algebraically closed.
Thus, $\alpha \in k$. This finishes Step 1.
Step 2: We show that $R = \mathrm{End}_k(E)$.
$R \subset \mathrm{End}_k(E)$ by hypothesis.
Suppose $A \in \mathrm{End}_k(E)$. Let $e_1, \cdots, e_n$ be a k-basis for $E = k^n$.
Density theorem implies: $\exists r \in R$ such that $Ae_i = re_i$ for all i.
Therefore, $A = r \in R$.

$\square$

Monday, 9/9/2024

Today:
Density Theorem
Characters determine representation
Artin-Wedderburn Theorem
Homework due Monday 9/16, Exercises 1-7
Recall Jacobson Density Theorem:
If E is semisimple over R, $e_1, \ldots, e_n \in E$ and $f \in R''$ then,

$$\exists r \in R \text{ s.t. } f(e_i) = re_i \forall i$$

Recall that R'' is defined as follows:

$$f \in R'' \iff f : E \to E \text{ s.t. } \forall \phi \in R' = \operatorname{End}_R E, f \circ \phi = \phi \circ f$$

Also recall Burnside's Theorem:
Suppose k is an algebraically closed field, and $k \subset R \subset M_n(k)$ are subrings
If k^n is a simple R-module, then
$R = M_n(k)$

3.7 Existence of Projection Operators

Theorem 17. Suppose $E = V_1 \oplus \cdots \oplus V_m$, simple non-isomorphic R-modules. Then, for any i, there exists $r_i \in R$ such that,

$$r_i v = \begin{cases} v, & \text{if } v \in V_i; \\ 0, & \text{if } v \in V_j, i \neq j \end{cases}$$

So, each projection map is just multiplication.

Proof. This is a consequence of the density theorem.
Choose nonzero $e_k \in V_k$.
Let $f = \pi_i : E \to E$ which is a projection on V_i.
Note that $f \in R''$ since for all $\phi \in R', \phi(V_k) \subset V_k$ [Schur's Lemma, non-isomorphic].
Density theorem $\implies \exists r_i \in R$ such that $r_i e_k = \pi_i(e_k)$.
Note that $V_k = Re_k$ so $\forall v \in V_k, v = re_k$.
So, $r_i v = r_i re_k = r\pi_i(e_k) = \pi_i(re_k) = \pi_i(v)$
Which is what we wanted.

□

Correction to the Existence of Projection Operators
Suppose k is a field, R is a k-algebra so that R is semisimple. Suppose R-module $E = V \oplus V', \dim_k E < \infty$.
For all simple $L \lhd V, \forall L' \lhd V'$ then $L \cong L'$
Then, $\exists r \in R$ such that for all $e \in E$,

$$re = \begin{cases} e, & \text{if } e \in V; \\ 0, & \text{if } e \in V'; \end{cases}$$

Proof. We apply density theorem. Since we have finite dimension, we have:

$$\{e_1, \cdots, e_n\} = (k\text{-basis of } V) \cup (k\text{-basis of } V')$$

Let $\pi_V : E \to E$ be the projection on V.
Then, $\pi_V \in R''$ [the second commutant] since $\forall \phi \in R', \phi(v) \subset V, \phi(v') \subset V'$.
Density theorem implies $\exists r$ such that $re_i = \pi_v(e_i)$.
Then $\forall a \in k \subset$ center R,
$r(ae_k) = a(re_k) = a\pi_v(e_k) = \pi_v(ae_k)$
Therefore, $re = \pi_v(re)$. □

Question: What is a k-algebra?
Following Atiyah-McDonald, let k be a commutative ring [often but not always a field]. Then,

$$R \text{ is a } k\text{-algebra} \overset{\text{def}}{\iff} \text{homomorphism } h : k \to R, h(k) \subset \text{center}(R)$$

Example. Any ring is a $\mathbb{Z}$-algebra, homomorphism sends n to $1 + 1 + \cdots + 1$
k field, $R \neq 0 \implies k \hookrightarrow R$
k-algebra $\iff k \subset \text{center}(R)$

Corollary 18 (3.8)**.** Suppose $\operatorname{char} k = 0$, R is a k-algebra, E, F semisimple over R, finite dimensional over k.
For $r \in R$, let:
$f_r^E : E \to E$ be $f_r^E(e) = re$
$f_r^F : F \to F$ be $f_r^F(f) = rf$
If $\operatorname{Tr}(f_r^E) = \operatorname{Tr}(f_r^F)$ for all $r \in R$,
Then $E \cong F$ as R-modules.

Proof. Let V be a simple R-module.
Suppose $E = V^n \oplus$ direct sum of simple R-modules not isomorphic to V
$F = V^m \oplus$ direct sum of simple R-modules not isomorphic to V
We want to show $n = m$
Let $r_v \in R$ be the projection operation from 3.7.
Then, $\operatorname{Tr}(f_{r_v}^E) = \operatorname{Tr}(r_v \cdot : E \to E) = \dim_k V^n = n \dim_k V$
Similarly, $\operatorname{Tr}(f_{r_v}^F) = m \dim_k V \implies n = m$

□

Corollary 19 (Characters determine representations)**.** Suppose k is a field and $\operatorname{char} k = 0$. Let G be a finite group. Suppose:
$\rho : G \to GL_n(k)$
$\rho' : G \to GL_m(k)$
with kG-modules $E = k^n$ over ρ and $F = k^m$ over ρ'
If $\operatorname{Tr}(\rho(g)) = \operatorname{Tr}(\rho'(g))$ for all g,
Then $E \cong F$ as kG-modules.
Note that, substituting $g = 1$ gives us:
$\operatorname{Tr}(\rho(1)) = \operatorname{Tr}(\rho'(1)) \implies \operatorname{Tr}(I) = \operatorname{Tr}(I) \implies n = m.$

Definition ((semi)simple rings)**.** Note that if R is a ring, then R is a left module as well. We write ${}_RR$ when we're considering it as a left module, and ${}_RR_R$ when we are considering a two sided ideal.
R is called a semisimple ring if ${}_RR$ is a semisimple R-module.
R is called a simple ring if R is a semisimple ring, and for all simple $L, L' \lhd_R R \implies L \cong L'$
This means, ${}_RR = \oplus_{i \in I} L_i$ where L_i are simple (left) ideals such that $L_i \cong L_j$ for all i, j.
Recall that an ideal is simple if it has no proper sub-ideals.

Example. $M_2(\mathbb{H})$ is a simple ring. We can write it as direct sum of two ideals

$$\begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$$

Example. $M_2(\mathbb{H}) \times \mathbb{R}$ is semisimple.

$$\begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix} \times 0 \oplus \begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix} \times 0 \oplus \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \times \mathbb{R}$$

Artin-Wedderburn generalizes this.

Theorem 20 (Artin-Wedderburn Theorem)**.** i) R simple $\iff R \cong M_n(D)$ where D is a skew-field.

ii) R semisimple $\iff R \cong R_1 \times \cdots \times R_s$ simple rings.

Wednesday, 9/11/2024

Today we discuss the Artin-Wedderburn Theorem.
Exercise: $C_2 = \{1, g\}$, prove that $\mathbb{Q}C_2$ is a semisimple ring.
$\mathbb{Q}C_2 = B_1 \oplus B_2$ 2-sided ideals
$\mathbb{Q}C_2 \cong \mathbb{Q} \times \mathbb{Q}$.

Lemma 21. Suppose we have a ring R which is decomposed as a sum of (left) ideals:

$$_RR = \bigoplus_{i \in I} L_i \quad \text{with } L_i \neq 0$$

Then $|I| < \infty$.

Proof. Suppose $_RR = \bigoplus_{j \in J} L_j$ where L_j are ideals. We want to prove that only finitely many are non-zero.
Note that, $1 = \sum_{j \in J} e_j$. We use only finitely many elements here, so $1 = \sum_{i \in I} e_i$ where $e_i \neq 0, I \subset J, |I| < \infty$.
For all $r \in R$ we have $r = r \cdot 1 = r \sum_{i \in I} e_i = \sum_{i \in I} re_i \in \sum_{i \in I} L_i$.
Therefore, $_RR = \bigoplus_{i \in I} L_i$ a finite sum! □

Now we go to the theorem.

Proof of Artin-Wedderburn Theorem Part I. We want to prove: R simple ring $\iff$ $R \cong M_n D$ where D is a skew field.
First, note that $_RR \cong L^n$ where L is a simple ideal [so no proper sub-ideals]. Therefore,

$$R^{op} \cong \mathrm{End}_R(_RR) \cong \mathrm{End}_R(L^n) \cong M_n(\underbrace{\mathrm{End}_R L}_{\text{division ring}})$$

Taking transpose,

$$R \cong M_n(\mathrm{End}_R L)^{op} \cong M_n((\mathrm{End}_R L)^{op}) = M_n(D)$$

So we are done with one direction!
The other direction is a exercise. Here are the steps:

Step 1: $M_n D = \begin{bmatrix} * & 0 & \cdots & 0 \\ * & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & 0 & \cdots & 0 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 0 & 0 & \cdots & * \\ 0 & 0 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{bmatrix}$

Step 2: Each summand is isomorphic to $D^n = \begin{bmatrix} * \\ * \\ \vdots \\ * \end{bmatrix}$

Step 3: D^n is a simple module.

□

Remark. R simple $\iff$ R artinian, R has no proper 2-sided ideals. Some definitions forgo the artinian condition, in this case these are called artinian simple rings.

Lemma 22 (4.2)**.** Suppose L is a simple ideal and M is a simple module so that $L \ncong M$. Then $LM = 0$.

Proof. This is a direct consequence of Schur's lemma. Consider the map $\phi_m : L \to M$ given by $l \mapsto lm$ for $m \in M$. Since this can't be an isomorphism, it must be the zero map. Thus, $lm = 0$. □

Proof of Artin-Wedderburn Theorem Part II. Idea: Decompose R as direct sum of simple ideals. Partition the set of simple ideals so that members of a partition are isomorphic to each other, members of a partition are not isomorphic to members of another partition. Direct sum of each partition gives us one R_j.
Suppose R is semisimple.
Let $L_1, \cdots, L_s$ be a set of pairwise non-isomorphic simple ideals [meaning $L_i \ncong L_j$]
So that, for all simple $L <_R R, L \cong L_i$ for some i.
Let $B_i = \sum_{L \cong L_i} L$.
Claim: B_i is a 2-sided ideal.
Proof of Claim:

$$B_i R \underset{4.2}{=} B_i B_i \subset R B_i \underset{B_i \text{ is a left ideal}}{=} B_i$$

Thus the claim is proven.
Claim: We have a 'block decomposition of R', meaning,
Proof of Claim:

$${}_R R_R = B_1 \oplus \cdots \oplus B_s$$

Subclaim: $B_i \cap \sum_{j \neq i} B_j = 0$
Proof of Subclaim: Every $r \in R$, we have that $r \in L$ where L is simple. $L \subset B_i \implies L \cong L_i$. $L \subset \sum_{j \neq i} B_j \implies L \cong B_j$ for some $j \neq i$ which is not possible.
Now, we go back to the main proof.
We can write $1 = e_1 + \cdots + e_s$.
Then, $R_i \coloneqq (B_i, e_i)$ is a ring!
We have $R \cong (R_1, e_1) \times \cdots \times (R_s, e_s)$, so we're done.
The other direction is an exercise.

□

Friday, 9/13/2024

Key idea:

$${}_R R = L^n \implies \operatorname{End}_R R \cong M_n(\operatorname{End}_R L)$$

Note that $R^{op} \cong \operatorname{End}_R R$ [function composition is written in the opposite direction].
Suppose $L_1, \cdots, L_s$ are non-isomorphic simple R-ideals.
L simple $\implies L \cong L_i$.
Define $B = \sum_{\text{simple } L \cong L_i} L \triangleleft_R R_R$.
We can prove that it is a two sided ideals.
Then we can write $R \cong R_1 \times \cdots R_s$ simple, where
$R_i = (B_i, e_i)$ [e_i is the identity in B_i].

Theorem 23 (4.4)**.** Suppose E is a R-module.

$$E_i \coloneqq \sum_{\substack{\text{simple } M \triangleleft E \\ M \cong L_i}} M$$

Then, $E = \bigoplus_{i=1}^{s} E_i$
$E_i = e_i E = B_i M$.

Corollary 24 (4.5)**.** If R is semisimple, M a simple R-module, then $M \cong L_i$ for some i.

Corollary 25 (4.6)**.** All simple modules of a simple ring are isomorphic.

$$M \cong \oplus L$$

External Product vs. Internal Product

Definition (External Product)**.** If we have [finite] rings $R_1, \cdots, R_s$ we can construct the ring:

$$R_1 \times R_2 \times \cdots \times R_s$$

Definition (Internal Product)**.** 'Block Decomposition': If we have a ring R and we can write it as sum of 2 sided ideals:

$$_R R_R = B_1 \oplus \cdots \oplus B_s$$

Then we have $e_j \in B_j$ so that:

$$1 = e_1 + \cdots + e_s$$

Then, each B_j has a ring structure with e_j as identity. Then,

$$R \cong (B_1, e_1) \times \cdots \times (B_s, e_s)$$

Just for clarity:

Definition (Direct Sum of Ideals)**.**

$$_R R_R = B_1 \oplus \cdots \oplus B_s$$

If and only if for every $r \in R$,

$$r = b_1 + \cdots + b_s$$

where $b_j \in B_j$ and the expression is unique.

Jim's Rant: A subring has to have the same identity. So, (B_j, e_j) is not a subring.
Block Decomposition is not a direct sum of rings!
This is because in category theory, sum refers to the co-product.

Lemma 26. Let k be a field, and let D be a skew-field which is a k-algebra such that $\dim_k D < \infty$. Then,

a) $\forall \alpha \in D$ we have $k[\alpha]$ is a field.

b) k algebraically closed $\implies D = k$.

Example. If $k \in \mathbb{R}, D = \mathbb{H}, \alpha \in \mathbb{H} - \mathbb{R}$ then $k[\alpha] \cong \mathbb{C}$.

It is not completely obvious since $k[i + j] \cong \mathbb{C}$ as well.

Proof. a) D is a k-algebra. Therefore, $k[\alpha]$ is commutative. We just need to find inverse.

Let $0 \neq \beta \in k[\alpha]$. It is enough to prove that for $\beta \in k[\alpha]$, multiplication map $\cdot\beta : k[\alpha] \to k[\alpha]$ is bijective.

$\cdot\beta$ is a finite dimensional linear transformation so those are true.

b) For all $\alpha \in D$ we have: $k[\alpha] = k$ since k is closed. So, $\alpha \in K$. Thus $D = k$. $\square$

Corollary 27. Suppose G is finite. Then,

$$\mathbb{C}G \cong \prod_{i=1}^{s} M_{n_i}(\mathbb{C})$$

Proof. Artin-Wedderburn Theorem plus the previous lemma. $\square$

Example. Suppose $C_n = \langle g \rangle$ cyclic and $\zeta_n = e^{2\pi i/n}$. Then,
$\mathbb{Q}C_2 \cong \mathbb{Q}_+ \times \mathbb{Q}_-$ where $g \mapsto (1, -1)$.
If p is prime we can write:
$\mathbb{Q}(C_p) \cong \mathbb{Q} \times \mathbb{Q}(\zeta_p)$ where $g \mapsto (1, \zeta_p)$.
$\mathbb{C}[C_n] \cong \mathbb{C}^n$ where:
$g \mapsto (1, \zeta_n, \cdots, \zeta_n^{n-1})$
$\mathbb{Q}[C_2 \times C_2] \cong \mathbb{Q}^4$ where:

$$(1, g) \mapsto (1, 1, -1, -1)$$

$$(g, 1) \mapsto (1, -1, 1, -1)$$

$\mathbb{R}[Q_8] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}$ where $\mathbb{R}[Q_8] \rightarrowtail \mathbb{R}[C_2 \times C_2]$
Some other examples: $\mathbb{Q}[C_n], \mathbb{C}[Q_8], \mathbb{Q}[D_{2n}], \mathbb{R}[D_{2n}], \mathbb{C}[D_{2n}]$

Representation Theory

Here, G is a finite group and k is a field.

Representations	Modules over kG	Characters
$\rho : G \to GL(V)$ where V is a finite dimensional vector space	V is a kG module	$\chi : G \to k, \chi_\rho(g) \operatorname{Tr} \rho(g)$

Table 1: Representations, Modules and Characters

Monday, 9/16/2024

We have:

$$\text{representation} \iff \text{modules over } kG \implies [\impliedby \text{ only if } \operatorname{char} k = 0] \text{ characters.}$$

rep $\to$ kG-module
$\rho \mapsto V_\rho$ by $(\sum_g a_g g)v \coloneqq \sum_g a_g \rho(g) v$
$\rho_v \leftarrow V$
$\rho_V(g)v \coloneqq gv$
Recall the definition of character:
We have the trace map:

$$\operatorname{Tr} : M_n k \to k$$

Where $\operatorname{Tr}(a_{ij}) = \sum_j a_{jj}$ [or the sum of eigenvalues]
We have $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$ which implies $\operatorname{Tr}(PAP^{-1}) = \operatorname{Tr}(A)$.
So, Tr is basis independent. Thus,

$$\operatorname{Tr} : \operatorname{End}_k V \to k$$

Definition (character)**.** Trace is an endomorphism map. This gives us:

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[rr, bend right, "\chi_p"'] & GL(V) \arrow[r, "\operatorname{Tr}"] & k \end{tikzcd}$$

This is called the <u>character of p</u>

There's a correspondence between kG modules and Representations concepts:

Repesentations	Modules over kG
irreducible	simple
	isomorphism
	direct sum
	Hom
	dual
	tensor product

Table 2: Rep and kG-mod

Irreducible vs Simple
We say irreducible representation, when we on the other hand say simple modules. Same concept!
Isomorphism
Suppose we have two representations:
$\rho : G \to GL(V)$
$\rho' : G \to GL(V')$
We say two representations are isomorphic when:

$$\rho \cong \rho' \overset{def}{\iff} V_\rho \overset{\phi}{\cong} V_\rho \overset{\phi}{\cong} V'_{\rho'} \underset{\phi(gv)=g\phi(v)}{\iff} \exists k \text{ isomorphism s.t.}$$

$\phi : V \to V'$ s.t. $\forall g \in G$ we have the following commutative diagram:

$$\begin{array}{ccc} V & \xrightarrow{\rho(g)} & V \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ V' & \xrightarrow{\rho'(g)} & V' \end{array}$$

ϕ is called the intertwining map.

Corollary 28. $\rho \cong \rho' \implies \chi_\rho = \chi_{\rho'}$

Direct Sum
Suppose $V \oplus W$ is a kG-module.

$$\rho_{V\oplus W} : G \to GL(V \oplus W)$$

is given by:

$$\rho_{V\oplus W} = \begin{bmatrix} \rho_V & 0 \\ 0 & \rho_W \end{bmatrix}$$

We also have $\chi_{V\oplus W} = \chi_V + \chi_W$.
Two Representations

Definition (Trivial Representations)**.**

$$\rho : G \to GL(k)$$

$$g \mapsto 1$$

Is the trivial representation. Also, $\chi_\rho \equiv 1$.

Definition (Regular Representation)**.** Consider the kG-module ${}_{kG}kG$. We have:

$$\rho_{kG} : G \to GL(kG)$$

This is injective.

Note that $G \curvearrowright G$ by multiplication, this is a free action. For finite group G with $|G| = n$,
$G \rightarrowtail$ Bijection(G, G) so G is a subgroup of S_n. So we have:

$$\begin{tikzcd} G \arrow[r] \arrow[rr, bend left, dotted, "\text{regular rep.}"] & S_n \arrow[r] & GL(k^n) \end{tikzcd}$$

With the action of 'permuting the standard basis'.
Exercise: Compute character of Regular Representation.
We have, in line of the previous theorem:

Theorem 29 (Maschke's Theorem)**.** If $V \subset W$ as kG-modules and $\operatorname{char} k \nmid |G|$ then $\exists V'$ such that $W = V \oplus V'$

Proof. First, find a k-linear map $\pi : W \to V$ such that $\pi(v) = v$ for all $v \in V$.
We average it to make it kG-linear:
$\pi' : W \to V$ given by:

$$\pi'(w) := \frac{\sum_g g\pi(g^{-1}w)}{|G|}$$

We have: π' is kG-linear and $\pi'(v) = v$
We can take $V' := \ker \pi$ □

Thus, for $w \in W$ we can write $w = \pi'(w) + (w - \pi'(w))$.
Note that Maschke's theorem implies kG is semisimple. Artin Wedderburn implies semisimple kG module is a direct sum of irreducible modules.

$$V \cong \bigoplus_i n_i V_i$$

$$\chi_V = \sum_i n_i \chi_i$$

Homomorphisms:
Suppose V, W are kG-modules, "representations". Then,
$\mathrm{Hom}_{kG}(V, W)$ is a k-vector space.
$\mathrm{Hom}_k(V, W)$ is a kG-module.
we define: $(gf)v := gf(g^{-1}v)$
i.e. $((\sum_g a_g g)f)v = \sum_g a_g(gf(g^{-1}v))$
The g^{-1} inside is needed for associativity: $(g'g)f = g'(gf)$
Officially this is a functor.
$\mathrm{Hom}_k(-,-) : (kG\text{-mod})^{op} \times kG\text{-mod} \to kG\text{-mod}$
Special case:
Dual Representation: $W = k$. Then,
$V^* = \mathrm{Hom}_k(V, k)$.
So, $(gf)(v) = gf(g^{-1}v) = f(g^{-1}v)$
Exercise: $\chi_{V^*} = ?$

Wednesday, 9/18/2024

Tensor Products

Motivation:
Product Structure: $- \otimes -$: kG-mod $\times kG$-mod $\to kG$-mod given by $V \otimes_k W$.
Group action works diagonally, $g(x \otimes y) = (gx) \otimes (gy)$, extended linearly.
Extension of scalars:

$$\mathbb{R}G \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}G$$

Product of Groups: $k[G \times H] = kG \otimes_k kH$

When for k a field then modules are vector spaces k^m and k^n which are easy:

$$k^n \otimes_k k^m = k^{nm}$$

$$\dim(k^n \otimes_k k^m) = mn$$

$\{e_i\}$ a basis for k^n
$\{f_j\}$ a basis for k^m
Then $\{e_i \otimes f_j\}$ is a basis for $k^n \otimes k^m$.
However, tensor product consists of more than 'pure' tensors.

Definition (Tensor Product)**.** Let R be a commutative ring. Tensor product is a functor:

$$- \otimes_R - : R - \text{mod} \times R - \text{mod} \to R - \text{mod}$$

$$(A, B) \mapsto A \otimes_R B$$

[Functor meaning if we have homomorphism on the left we will have homomorphisms on the right]
Construction:
Let $F(A \times B)$ be the free R-module with basis $A \times B$. Then a typical element of the basis is $(a, b) \in A \times B$.
Let S be the sub-module generated by the following:

1) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$
2) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$
3) $r(a, b) - (ra, b)$
4) $r(a, b) - (a, rb)$

Then, we define:

$$A \otimes_R B \coloneqq \frac{F(A \times B)}{S}$$

and write $a \otimes b$ for the image of (a, b).
This means, a typical element of $A \otimes_R B$ is:

$$\sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_R B$$

We also have the following relations:
$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \times b$
$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$
$r(a \otimes b) = (a \otimes rb) = (ra \otimes b)$

Exercise. $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$

Proposition 30. Suppose A, B, M are R-modules, and

$$\phi : A \times B \to M \text{ is } R\text{-billinear}$$

Meaning,

1) $\phi(a_1 + a_2, b) = \phi(a_1, b) + \phi(a_2, b)$
2) $\phi(a, b_1 + b_2) = \phi(a, b_1) + \phi(a, b_2)$
3) $r\phi(a, b) = \phi(ra, b) = \phi(a, rb)$

Then, by definition,

$$\pi : A \times B \to A \otimes_R B$$

is R-bilinear.

Proposition 31 (Universal Property of Tensor Product)**.** π is initial in the category of bilinear maps with domain $A \times B$. Meaning, every bilinear map from $A \times B$ factors through π.

$$\begin{tikzcd} A \times B \arrow[r, "\forall\phi \text{ bilinear}"] \arrow[d, "\pi"] & M \\ A \otimes_R B \arrow[ur, dotted, "\exists!\overline{\phi}"'] & \end{tikzcd}$$

This diagram commutes

Proof. For uniqueness, note that, $\overline{\phi}(a \otimes b) = \overline{\phi}(\pi(a, b)) = \phi(a, b)$
For existence, define $\hat{\phi}(a, b) = \phi(a, b)$ where $\hat{\phi} : F(A \times B) \to M$. Then $\overline{\hat{\phi}}(S) = 0$ so $\overline{\phi} : A \otimes_R B \to M$ exists. ☐

Proposition 32 (Rephrasing Universal Property in Terms of Adjoint Functors)**.**

$$\mathrm{Hom}(A \otimes B, C) \cong \mathrm{Hom}(A, \mathrm{Hom}(B, C))$$

Proof.

$$f \mapsto (a \mapsto (b \mapsto f(a \otimes b)))$$

$$(a \otimes b \mapsto g(a)b) \leftarrow g$$

$$\begin{tikzcd} R\text{-mod} \arrow[r, bend right, "\mathrm{Hom}(A, \mathrm{Hom}(-,C))"'] & R\text{-mod} \arrow[l, bend right, "\mathrm{Hom}(A\otimes -, C)"'] \end{tikzcd}$$

☐

Proposition 33. 1) Commutative $A \otimes_R B \cong B \otimes_R A$

2) Identity $R \otimes_R B \cong B$

3) Assocative $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$

4) Distributive $(\bigoplus_\alpha A_\alpha) \otimes B \cong \bigoplus_\alpha (A_\alpha \otimes B)$

5) Functorial $\begin{pmatrix} f : A \to A' \\ g : B \to B' \end{pmatrix} \implies \quad f \otimes g : A \otimes B \to A' \otimes B'$

6) Exactness Short Exact Sequence $0 \to A \xrightarrow{f} B \to C \to 0 \implies$ Short Exact Sequence $0 \to A \otimes M \xrightarrow{f \otimes 1_M} B \otimes M \to C \otimes M \to 0$

7) Right Exactness M R-mod,$0 \to A \to B \to C \to 0 \implies$ Exact Sequence $A \otimes M \to B \otimes M \to C \otimes M \to 0$

Friday, 9/20/2024

Lang Section 2

Tensor Product of Representation
Suppose V, W are k-vector spaces, then we have $V \otimes_k W$ is also a k-vector space. But they all are kG-modules as well:

$$g(v \otimes w) = gv \otimes gw$$

Proposition 34. The character is multiplicative:

$$\chi_{v \otimes w} = \chi_v \chi_w$$

Proof. Let $\{e_i\}$ be a basis for V and $\{f_j\}$ a basis for w.
Suppose $ge_i = \sum_k a_{ki} e_k$
And $gf_j = \sum_l b_{lj} f_l$
Then, $g(e_i \times f_j) = ge_i \times gf_j = \sum_{k,l} e_{ki} b_{lj} e_k \times f_l$
Take $(k, l) = (i, j)$.
Then, $\chi_{v \times w}(g) = \sum_{i,j} a_{ii} b_{jj} = \chi_v(g) \chi_w(g)$ $\square$

Consider $f : G \to k$. We have:
$\{$1d chars$\} \subset \{$simple chars$\} \subset \{$chars$\} \subset \{$virtual chars$\} \subset \{$class functions$\}$
We explain these later.

Definition. f is a character if $\exists \rho : G \to GL_k(V)$ such that $f = \chi_\rho = \operatorname{Tr} \circ \rho$

Definition. f is a class function if $\forall g, h \in G$ we have $f(hgh^{-1}) = f(g)$

Definition. f is a virtual character if $\exists \rho, \rho'$ such that $f = \chi_\rho - \chi_{\rho'}$

Definition. f is simple (=irreducible) character if $f = \chi_V$ where V is a simple kG-module.

Definition. f is 1-dimensional character if $f : G \to k^\times$ is a homomorphism. eg trivial character $\chi_1(g) \equiv 1$.

Proposition 35. Class Functions are k-algebras. Virtual characters are a commutative ring.

Now, suppose $\operatorname{char} k \nmid |G|$. Then,

$$kG \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$$

Assume $M_{n_1}(D_{n_1}) = k$. Then we have the trivial representation: $ga = a$.
If $L_i = D_i^{n_i}$ is a simple kG-module, then
$\chi_i = \chi_{L_i}$ is a simple characteristics.
We have $1 = e_1 + \cdots + e_s$ [central non-trivial idempotents].
$\chi_i(e) = \operatorname{Tr}(\operatorname{Id}_{L_i}) = \dim_k L_i = n_i \dim_k D_i$.

Example. Consider $Q_8 \hookrightarrow \mathbb{H}^\times$. Then,

$$\chi_{\mathbb{H}}(e) = 4$$

Now, consider ${}_{kG}kG \cong \bigoplus_i n_i L_i$, the 'regular representation'. $e_j L_i = 0$ for $i \neq j$. Then,

$$\chi_i(e_i) = \chi_i(1) = \chi_i(e) = \dim_k L_i$$

So, char $\chi : G \to k$ extends to $\chi : kG \to k$ by $\sum a_g g \mapsto \sum a_g \chi(g)$.
If V is a finitely generated kG-module, we have

$$V \cong m_1 L_1 \oplus \cdots \oplus m_s L_s$$

where $m_i \geq 0$.

Theorem 36 (2.2, 2.3)**.** $\chi_v = \sum_i m_i \chi_i : G \to k$ with m_i uniquely determined if $\operatorname{char} k = 0$.

Theorem 37 (2.3)**.** Characters Determine Representations: suppose $\operatorname{char} k = 0$. Then,

$$V \cong V' \iff \chi_V = \chi_{V'}$$

Proof. $\implies$: Trace is independent of basis, so this is easy.
$\impliedby$: We already gave a proof using projection operators. Second Proof:
Assume $\chi_V = \chi_{V'}$. We decompose:

$$V \cong \oplus m_i L_i, V' \cong m_i' L_i$$

Note that we have $\chi_V(e_i) = m_i \dim_k L_i = m_i' \dim_k L_i = \chi_{V'}(e_i)$
Thus we must have $m_i = m_i'$. ☐

Representation Ring

$R_k(G) = (\text{virtual char}, +, \times) \cong (\text{virtual rep}, \oplus, \otimes)$.
Example: $R_{\mathbb{Q}}[C_2] \cong \frac{\mathbb{Z}[X]}{(X^2-1)}$

Monday, 9/23/2024

Dual Characters

Consider $\rho : G \to GL_k(V)$
Dual $V^* = \operatorname{Hom}_k(V, k)$ is also a representation.

$$(g\phi)(v) = \phi(g^{-1}v)$$

Inverse because we want it to be a left module.
Claim: $\rho : G \to GL(V) \to \rho^* : G \to GL(V^*)$
$\rho^*(g) = (\rho(g)^{-1})^T$

Proof. $\rho^*(g) = (\rho(g^{-1}))^* = \rho(g^{-1})^T$ ☐

Corollary 38. a) $\chi_{V^*}(g) = \chi_v(g^{-1})$

b) $\chi_{\operatorname{Hom}(V,W)}(g) = \chi_V(g^{-1})\chi_W(g)$

Proof. a follows from the claim.
b: Consider the slant homomorphism:

$$V^* \otimes W \to \operatorname{Hom}(V, W)$$

$$\sum_i \phi_i \otimes w_i \mapsto \left(v \mapsto \sum_i \phi_i(v) w_i \right)$$

It is an isomorphism since V, W are both finite dimensional.

$$\chi_{\operatorname{Hom}(V,W)}(g) = \chi_{V^* \otimes W}(g) = \chi_{V^*}(g)\chi_W(g) = \chi_V(g^{-1})\chi_W(g)$$

☐

1 Dimensional Characters

Definition. 1 D representation is a homomorphism $\rho : G \to k^\times$

$$\begin{tikzcd} G \arrow[rr] \arrow[dr] & & k^\times \\ & G^{ab} \arrow[ur] & \end{tikzcd}$$

Question: What are the 1d representations for D_6?
$D_6 \cong \mathbb{Z}/3 \rtimes \mathbb{Z}/2$
So, $D_6^{ab} \cong \mathbb{Z}/2$
So, we have k_T, k_-
$r \mapsto 1$
$s \mapsto -1$
Exercise: Trivial Representation / Idempotent

$$e_T = \frac{\sum_{g\in G} g}{|G|} \in kG$$

$$e_T^2 = e_T$$

$$ge_T = e_T = e_T g$$

$$e_T \in Z(kG)$$

$$kG = (kG)e_T \oplus (kG)(1 - e_T)$$

$$kG \cong k \times \frac{kG}{\langle e_T \rangle}$$

Lemma 39 (2)**.** Any finite subgroup of $k^\times$ is cyclic.

Proof. Key Fact: $x^e - 1 \in k[x]$ has at most e roots [proof: long division].
Note: $x^2 - 1 \in \mathbb{Z}/8[x]$ has 4 roots. This implies $\mathbb{Z}/8$ is not a field.
Consider finite abelian $A < k^\times$
Consider $e =$ exponent $A = \inf\{m \geq 1 \mid \forall a \in A, a^m = e\}$
Then, $\forall a \in A, a^e - 1 = 0$. From the key fact, $|A| \leq e \leq |A|$
Thus, $e = |A|$ □

Corollary 40. $\forall$ hom $\quad \rho : G \to k^\times, \exists$ Cyclic C such that:

$$\begin{tikzcd} G \arrow[rr, "\rho"] \arrow[dr, two heads] & & k^\times \\ & C \arrow[ur, tail] & \end{tikzcd}$$

Recall only finite subgroup of $\mathbb{Q}$ is ± 1.
$1 - d$ $\mathbb{Q}$ reps of $G \leftrightarrow$ trivial representation + index 2 subgroups
Now we suppose k is algebraically closed, eg $k = \mathbb{C}$. Then,

$$kG \cong \prod_i M_{n_i}(k)$$

If G is abelian, then,

$$kG \cong k \times \cdots \times k$$

Corollary 41 (3)**.** k is algebraically closed and G is abelian $\iff$ all irreducible representations are 1-dimensional.

Corollary 42. Let $|G| = n, k = \mathbb{C}$.

a) $\forall V, \chi_V(G) \subset \mathbb{Q}(\zeta_n)$

b) $\forall V, \chi_{V^*}(g) = \overline{\chi_V(g)}$

c) $\forall V, W, \chi_{\mathrm{Hom}(V,W)}(g) = \overline{\chi_V(g)}\chi_W(g)$

Proof. a) True for 1d representation from the lemma.
$\implies$ True for G abelian (corollary 3)
$\implies$ True for cyclic G
$\implies$ always true: $g \in G \implies \langle g \rangle$ cyclic.

$$\chi_\rho(g) = \chi_{\rho|_{\langle g \rangle}}(g)$$

Then, $\rho : G \to GL(V)$, consider $g \in G$.
Then $\rho(g)^n = I \implies \mathrm{Tr}(\rho_V(g)) \in \mathbb{Q}(\zeta_n)$.

b) Same as (a).
$\rho^*(g) = (\rho(g)^{-1})^t$
For 1-dim, $\rho^* = \overline{\rho}$.

c) $\chi_{\mathrm{Hom}(V,W)}(g) = \chi_V(g^{-1})\chi_W(g) = \overline{\chi_V(g)}\chi_W(g)$

□

Two Bases for center kG

Definition. $g \in G$ is conjugate to $\sigma \in G$ if $\exists \tau$ such that,

$$\tau g \tau^{-1} = \sigma$$

Write $g \sim \sigma$

$G = \coprod_{G/\sim} [g]$
$[g] = \{\sigma \in G \mid g \sim \sigma\}$ conjugacy classes

Proposition 43. $\{\sum_{\sigma \in [G]} \sigma\}_{[g] \in G/\sim}$ is a k-basis for center of kG.

Proof. Clearly these are linearly independent.
$\alpha = \sum_{\sigma \in G} a_\sigma \sigma \in$ center
$\iff \tau\alpha = \alpha\tau \iff \tau\alpha\tau^{-1} = \alpha$
$\sigma a_\sigma \tau\sigma\tau^{-1} = \sum a_\sigma \sigma \implies (g \sim \sigma \implies a_g = a_\sigma)$

□

Wednesday, 9/25/2024

Lang XVIII, 4
Two bases for $Z(kG)$
conjugacy classes
primitive cental idempotents [k algebraically closed]

Exercise. $G \rightarrowtail Q$, prove that $kG \cong kQ \times R$

Proposition 44 (4.1)**.** Suppose $\{\sum_{\sigma \in [g]}\}_{[g] \in G/\sim}$ form a $\{^{k}_{\mathbb{Z}}\}$-basis for $\{^{Z(kG)}_{Z(\mathbb{Z}G)}\}$

Consider a ring R.

Definition. $e \in R$ is a primitive central idempotent if:
e is a central idempotent $[e^2 = e, e \in Z(R)]$
$e = e' + e''$ with e', e'' central idempotent $\implies \{e', e''\} = \{0, e\}$

Then, $kG \ni 1 = e_1 + \cdots + e_s, kG \cong \prod M_{d_i}(D_i)$
$e_i \to (0, \cdots, 0, 1, 0, \cdots, 0)$
Now suppose $n = |G|$
We have irreducible representations $L_1, \cdots, L_s$ and degrees $d_1, \cdots, d_s$ then $L_i \cong D_i^{d_i}$. We have irreducible characteristics $\chi_1, \cdots, \chi_s$ and primitive central idempotents (p.c.i.) $e_1, \cdots, e_s$
Facts: $(*)$: ${}_{kG}kG = \bigoplus_i d_i L_i$
$(**)$: $\alpha \in kG, i \neq j$ then $\chi_j(e_i\alpha) = 0$ since $e_i L_j = 0, \chi_i(e_i\alpha) = \chi_i(1\alpha) = \chi_i(\alpha)$
We have: $\chi_{\text{reg}} = \sum_i d_i \chi_i$

Proposition 45 (4.3)**.** $\chi_{\text{reg}}(g) = \begin{cases} n, & \text{if } g = e; \\ 0, & \text{if } g \neq e \end{cases}$

Proof. $\chi_{\text{reg}}(g) = \text{Tr}(\cdot g : kG \to kG)$
Thus, $\chi_{\text{reg}}(e) = \text{Tr}(I) = n$
If $g \neq e$ note that G has $\{\sigma_1, \cdots, \sigma_n\}$ and $\rho_{\text{reg}}(g)(\sigma_j) = g\sigma_j \neq \sigma_j$ for all j. So, there is nothing in the diagonal matrix and trace is 0. $\square$

Motivation for k algebraically closed:
Consider $\mathbb{Q}C_3 \cong \mathbb{Q} \times \mathbb{Q}(\zeta_3)$. We only have primitive central idempotents, $1 = e_1 + e_2$.
But the center has dimension 3: $\dim_{\mathbb{Q}}(Z(\mathbb{Q}C_3)) = 3$.
Assume k is algebraically closed.
Claim: k algebriacally closed, D skew field, $k < Z(D)$, $\dim_k D < \infty$ implies $k = D$
Now, $kG \neq \prod M_{d_i}(k)$
Consider primitimve central idempotents $e_1, \cdots, e_s$ for a basis.
$n = \sum_{i=1}^s d_i^2$
e.g. $S_3 = D_6$. $s =?$ $d_1, d_2, d_3 =?$
We have represantatives of conjugacy classes: $(1), (12), (123)$.
$s = 3, 6 = 1^2 + 1^2 + 2^2$
Char. Table:

	(1)	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Table 3: characteristic table

We have $\mathbb{C}S_3 = \mathbb{C}_+ \times \mathbb{C}_- \times M_2\mathbb{C}$
Our representatives are $(1), (12), (123), (1234), (12)(34)$
$d_i = 1, 1, 2, 3, 3$
Goal: Express the p.c.i basis in terms of conjugacy class basis.

Corollary 46 (4.2)**.** If k is algebraically closed,
the number of conjugacy classes $= \dim_k Z(G) =$ number of irreducible representation $= s$

Proposition 47 (4.4)**.** k algebraically closed, then

$$e_i = \frac{d_i}{n} \sum_{\tau \in G} \chi_i(\tau^{-1})\tau$$

Proof. Let $e_i = \sum_{\tau \in G} a_\tau \tau$.
We compute $\chi_{\text{reg}}(e_i\tau^{-1})$ in two ways.
1: $\chi_{\text{reg}}(e_i\tau^{-1}) = \chi_{\text{reg}}(\sum a_\sigma \sigma\tau^{-1}) = \sum a_\sigma \chi_{\text{reg}}(\sigma\tau^{-1}) = a_\tau n$
2: $\chi_{\text{reg}}(e_i\tau^{-1}) \overset{(*)}{=} \sum_j d_j\chi_j(e_i\tau^{-1}) \overset{(**)}{=} d_i\chi_i(e_i\tau^{-1}) = d_i\chi_i(\tau^{-1})$
Thus, $a_\tau n = d_i\chi_i(\tau^{-1}) \implies a_\tau = \frac{d_i}{n}\chi_i(\tau^{-1})$ $\square$

Corollary 48 (4.5)**.** Let $m = \exp G$. Then,

$$e_i \in \frac{1}{n}\left[\mathbb{Z}[\zeta_m]G\right] \subset \frac{1}{n}\left[\mathbb{Z}[\zeta_n]G\right]$$

Corollary 49 (4.6)**.** $\operatorname{char} k \nmid d_i$

Proof. If not, $\operatorname{char} k \mid d_i$ then $e_i = 0$ which is a contradiction. □

Corollary 50 (4.7)**.** $\chi_1, \cdots, \chi_s$ are linearly independent over k. In fact they form a basis for the class functions $f : G \to k$.

Proof. Suppose $0 = \sum a_i\chi_i$.
Then $0 = \sum a_i\chi_i(e_j) = a_j\chi_j(e_j) = a_jd_j \implies a_j = 0$ □

Then $\dim_k$(class functions) = number of conjugacy classes = s.

Friday, 9/27/2024

Review:

$$e_i = \frac{d_i}{n}\sum_{\sigma\in G}\chi_i(\sigma)\sigma^{-1} \in kG \quad (*)$$

Is a primitive central idempotent.

$$\chi_{\text{reg}} = \chi_{kG} = \sum_i d_i\chi_i$$

$\sigma = 1, n = \sum_i d_i^2$
$d_i \mid n$

$$\sum_{\sigma\in G}\chi_i(\sigma)\chi_j(\sigma^{-1}) = n\delta_{ij}$$

$$\sum_{i=1}^{s}\chi_i(\sigma)\chi_i(\tau^{-1}) = \begin{cases} \frac{n}{|\sigma|}, & \text{if } \tau = \sigma; \\ 0,` & \text{otherwise.}\end{cases}$$

If $G = S_3$ then:

	(1)	(12)	(123)	
χ_1	1	1	1	6
χ_2	1	-1	1	6
χ_3	2	0	-1	6
	6	2	3	

Table 4: Characeristic Table of S_3

$0 = \chi_{\text{reg}}(123) = 1\chi_1(123) + 1\chi_2(123) + 2\chi_3(123)$
$k = \mathbb{C}, \chi(\sigma^{-1}) = \overline{\chi(\sigma)}$
End of review
$X(G) = \{\text{class functions } f : G \to k\}$ so that $f(\tau\sigma\tau^{-1}) = f(\sigma)$.

Definition (Perfect Pairing)**.** A perfect pairing of k vector space is a k-bilinear map $\beta : V \times W \to k$ such that $\exists$ basis $\{v_i\}, \{w_j\}$ such that

$$\beta(v_i, w_j) = \delta_{ij}$$

$$\iff \operatorname{Ad}_b : V \to W^*$$

$$v \mapsto (w \mapsto \beta(v, w))$$

Theorem 51 (4.9)**.**
$$X(G) \times Z(kG) \to k$$

$$(f, \alpha) \mapsto f(\alpha)$$

is a perfect pairing.

Proof. Dual basis: $\left\{\frac{1}{d_i}\chi_i\right\}, \{e_j\}$

$$\frac{1}{d_i}\chi_i(e_j) = \delta_{ij}$$

□

Corollary 52 (4.8)**.** Suppose k is algebraically closed, $\operatorname{char} k = 0$. Then $d_i = \dim_K L_i \mid n$

We need integrality theory (M502)
See Lang p 334.
A subring of B, $\alpha \in B$.
α is integral over A if $\exists$ monic $f(x) \in A[x]$ such that $f(\alpha) = 0$.
$\alpha \in \mathbb{Q} \implies \alpha \text{ int}/\mathbb{Z} \iff \alpha \in \mathbb{Z}$
Condition $(**)$: α being integral is equivalent to the existence of a faithful $A[\alpha]$-module M which is finitely generated as A-module.
Faithful means: $\forall \beta \in A[\alpha], \beta M = 0 \iff \beta = 0$.
In other words, $A[\alpha] \hookrightarrow \operatorname{End}_{A[\alpha]}(M)$.
Condition $(**) \iff \alpha \text{ int}/A$. This is proved by a determinant trick.
Applying $(**)$ on $A = \mathbb{Z}$, $\frac{n}{d_i} \in \mathbb{Q}$,
Multiplying $e_i = \frac{d_i}{n}\sum_{\sigma \in G}\chi_i(\sigma)\sigma^{-1} \in kG$ with e_i,

$$e_i = e_i^2 = \frac{d_i}{n}\sum_{\sigma}\chi_i(\sigma)\sigma^{-1}e_i$$

$$\frac{n}{d_i}e_i = \sum_{\sigma}\chi_i(\sigma)\sigma^{-1}e_i$$

$$M = \mathbb{Z}\langle\zeta_n^j\sigma e_i\rangle_{j,\sigma\in G} \text{ is a } \mathbb{Z}\left[\frac{n}{d_i}\right]\text{-module}$$

We are done by $(**)$. $d_i \mid n$.

Orthogonality, Lang XVIII, 5, Serre 2.3

Theorem 53. Suppose we have $\langle , \rangle : X(G) \times X(G) \to k$ by:

$$\langle f, g\rangle = \frac{1}{n}\sum_{\sigma\in G} f(\sigma)g(\sigma^{-1})$$

is a nonsingular symmetric form and $\{\chi_1, \cdots, \chi_s\}$ forms an orthonormal basis.

Proof. Symmetric form, k-bilinear $\langle f, g\rangle = \langle g, f\rangle$
Apply χ_j to $(*)$

$$d_i\delta_{ij} = \chi_j(e_i) = \frac{d_i}{n}\sum_{\sigma}\chi_i(\sigma)\chi_j(\sigma^{-1})$$

□

Remark: Irreducibility criterion: $\langle\chi, \chi\rangle = 1 \iff \chi$ irreducible.
$(\sum_i a_i\chi_i, \sum_i a_i\chi_i) = \sum_i a_i^2$

Proposition 54 (I.7, Serre p20)**.** a) $\sum_{i=1}^{s}\chi_i(\sigma)\chi_i(\sigma^{-1}) = \frac{n}{|[\sigma]|}$

b) $[\sigma] \neq [\tau] \implies \sum_{i=1}^{s}\chi_i(\sigma)\chi_i(\tau^{-1}) = 0$

Proof. Consier the characteristic function for $[\sigma]$:
$f_\sigma = 1$ on $[\sigma]$ and 0 everywhere else.
$f_\sigma = \sum_i \lambda_i \chi_i$.
$\lambda_j = \langle f_\sigma, \chi_j \rangle = \frac{1}{n} \sum_{\tau \in G} f_\sigma(\tau) \chi_j(\tau^{-1}) = \frac{|[\sigma]|}{n} \chi_j(\sigma^{-1})$
$f_\sigma(-) = \sum_i \frac{|[\sigma]|}{n} \chi_i(\sigma^{-1}) \chi_i(-)$ $\square$