Group representations 1

Some examples; Maschke's theorem

March 15, 2021

Representations of $\mathbb{Z}_n$ over $\mathbb{C}$

Example

Describe all (matrix) representations of $\mathbb{Z}_n$ over $\mathbb{C}$ of finite degree.

Let us start with matrix representations. Let $G := \mathbb{Z}_n$. We have to find $\mathrm{Hom}(G, \mathrm{GL}(d, \mathbb{C}))$ for every $d \in \mathbb{N}$. Recall that

$$\mathrm{Hom}(G, \mathrm{GL}(d, \mathbb{C})) \leftrightarrow \{A \in \mathrm{GL}(d, \mathbb{C}) \mid A^n = E\}$$

$$\psi \mapsto \psi(1)$$

We have to find matrices satisfying $A^n = E$. Recall every matrix is similar to a matrix in Jordan canonical form. From this we see that A has to be diagonalizable.
That is, there exists $X \in \mathrm{GL}(d, \mathbb{C})$ such that

$$XAX^{-1} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_d)$$

where $\lambda_1, \ldots, \lambda_d$ are complex numbers satisfying
$\lambda_t^n = 1, t = 1, \ldots, d$.

Representations of $\mathbb{Z}_n$ over $\mathbb{C}$, cont.

Let ψ_A be the matrix representation corresponding to A, i.e.,

$$\psi_A(g) = A^g, g \in G = \mathbb{Z}_n$$

. Then ψ_A is equivalent to $\psi_{XAX^{-1}}$ since for every $g \in G$

$$X\psi_A(g)X^{-1} = XA^g X^{-1} = (XAX^{-1})^g = \psi_{XAX^{-1}}(g)\,.$$

Notice that $\psi_{XAX^{-1}}(g) = \mathrm{diag}(\lambda_1^g, \lambda_2^g, \ldots, \lambda_d^g)$.
If $\psi_t \colon G \to \mathrm{GL}(1, \mathbb{C}) =: \mathbb{C}^*$ is given by $\psi_t \colon g \mapsto \lambda_t^g$, then
$\psi_{XAX^{-1}} = \psi_1 \oplus \psi_2 \oplus \cdots \oplus \psi_d$
Overall we proved that every matrix representation of $\mathbb{Z}_n$ over $\mathbb{C}$ is equivalent to a direct sum of representations of degree 1.

When are direct sums equivalent?

Now consider two families of degree one representations of $G = \mathbb{Z}_n$ over $\mathbb{C}$.

$$\psi_1, \psi_2, \ldots, \psi_d, \psi'_1, \psi'_2, \ldots, \psi'_d \colon G \to \mathrm{GL}(1, \mathbb{C})\,.$$

We wonder when $\psi := \psi_1 \oplus \cdots \oplus \psi_d$ and $\psi' := \psi'_1 \oplus \psi'_2 \oplus \cdots \oplus \psi'_d$ are equivalent.
Let $\lambda_t := \psi_t(1)$ and $\lambda'_t := \psi'_t(1)$ for every $1 \leq t \leq d$.
If ψ and ψ' are equivalent, then $\psi(1)$ and $\psi'(1)$ are similar matrices. Now $\lambda_1, \lambda_2, \ldots, \lambda_d$ are the eigenvalues of $\psi(1)$ and $\lambda'_1, \lambda'_2, \ldots, \lambda'_d$ are the eigenvalues of $\psi'(1)$.
More precisely $(-1)^d(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_d)$ is the characteristic polynomial of $\psi(1)$ and $(-1)^d(x - \lambda'_1)(x - \lambda'_2) \cdots (x - \lambda'_d)$ is the characteristic polynomial of $\psi'(1)$.

Since equivalent matrices have equal characteristic polynomials, ψ is equivalent to ψ' only if there exists a permutation $\sigma \in S_d$ such that

$$\lambda_t = \lambda'_{\sigma(t)}; t = 1, 2, \ldots, d$$

This condition is easily seen to be equivalent to $\psi_t = \psi_{\sigma(t)}$ for each $t \in \{1, 2, \ldots, d\}$.

On the other hand, if $\psi_t = \psi_{\sigma(t)}$ for each $t \in \{1, 2, \ldots, d\}$ is true for some $\sigma \in S_d$, then ψ and ψ' are equivalent.

The same result in the category $\mathrm{Rep}_{\mathbb{C}}(\mathbb{Z}_n)$

We still assume $G = \mathbb{Z}_n$. Let us translate previous result on matrix representations of G over $\mathbb{C}$ to the language of $\mathrm{Rep}_{\mathbb{C}}(G)$.
Let $\varphi \colon G \to \mathrm{Aut}_{\mathbb{C}}(V)$ be a homomorphism where $\dim_{\mathbb{C}}(V) = d$ is finite. Then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_d$, where $V_1, V_2, \ldots, V_d$ are φ-invariant subspaces of dimension 1.
We know that $\varphi(1)$ is diagonalizable. Let $B = \{b_1, b_2, \ldots, b_d\}$ be a basis of V such that $[\varphi(1)]_B$ is diagonal. Let $\lambda_i \in \mathbb{C}$ be the eigenvalue of $\varphi(1)$ related to b_i, that is, $[\varphi(1)](b_i) = \lambda_i b_i$.
Then $V_i := \langle b_i \rangle$ is φ-invariant, as $[\varphi(g)](b_i) = \lambda_i^g b_i$ for every $g \in G$.
Then φ is equivalent to $\varphi_{V_1} \oplus \varphi_{V_2} \oplus \cdots \oplus \varphi_{V_d}$.

The same result proved in $\mathbb{C}\mathbb{Z}_n$-Mod (outline)

We want to understand modules over $\mathbb{C}\mathbb{Z}_n$.
We want to use the isomorphism $\mathbb{C}\mathbb{Z}_n \simeq \mathbb{C}[x]/(x^n - 1)$ of $\mathbb{C}$-algebras. In this isomorphism $\delta_g \leftrightarrow \overline{x}^g$.
Let $\lambda_0, \ldots, \lambda_{n-1}$ be the roots of $x^n - 1$, say

$$\lambda_t = e^{\frac{2\pi \mathrm{i}}{n} t}, t \in \{0, 1, \ldots, n-1\}$$

Every $\mathbb{C}[x]/(x^n - 1)$-module has a canonical structure of a $\mathbb{C}\mathbb{Z}_n$-module (and vice versa). For example, if M is a $\mathbb{C}[x]/(x^n - 1)$-module, then the corresponding $\mathbb{C}\mathbb{Z}_n$-module M satisfies

$$\delta_g m = \overline{x}^g m, g \in \mathbb{Z}_n, m \in M .$$

CRT

The Chinese reminder theorem gives another isomorphism of $\mathbb{C}$-algebras:

$$\mathbb{C}[x]/(x^n - 1) \simeq \prod_{t=0}^{n-1} \mathbb{C}[x]/(x - \lambda_t) = \mathbb{C}^n$$

In general, modules over a product of rings $R \times S$ are constructed as follows: Take an R-module M and an S-module N and define an $R \times S$-module on the abelian group $M \oplus N$ in an obvious way

$$(r, s)(m, n) := (rm, sn), (r, s) \in R \times S, (m, n) \in M \oplus N\,.$$

And every $R \times S$-module is isomorphic to a module constructed this way.
A similar construction applies to modules over finite product of rings.

Putting these things together

The structure of modules over $T := \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C} = \mathbb{C}^n$ is easy: Take $V_1, V_2, \ldots, V_n$ vector spaces over $\mathbb{C}$. Define $V := V_1 \oplus V_2 \oplus \cdots \oplus V_n$ a T-module structure on V by

$$(c_1, c_2, \ldots, c_n).(v_1, v_2, \ldots, v_n) := (c_1 v_1, c_2 v_2, \ldots, c_n v_n)$$

for every $(c_1, \ldots, c_n) \in T$ and $(v_1, \ldots, v_n) \in V$.
Since we know $\mathbb{C}\mathbb{Z}_n \simeq T$ via

$$\delta_g \mapsto (\lambda_0^g, \lambda_1^g, \ldots, \lambda_{n-1}^g)$$

the $\mathbb{C}\mathbb{Z}_n$-module structure on V is defined by

$$\delta_g(v_1, v_2, \ldots, v_n) = (\lambda_0^g v_1, \lambda_1^g v_2, \ldots, \lambda_{n-1}^g v_n)$$

Again we see that this module is a direct sum of its submodules which have over $\mathbb{C}$ dimension 1.

Representations of $\mathbb{Z}_3$ over $\mathbb{Q}$

Example

Find representations of $\mathbb{Z}_3$ over $\mathbb{Q}$.

Use the following isomorphisms of $\mathbb{Q}$-algebras:

$$\mathbb{Q}\mathbb{Z}_3 \simeq \mathbb{Q}/(x^3 - 1) \simeq \mathbb{Q} \times \mathbb{Q}[x]/(x^2 + x + 1)$$

The product on the right hand side gives us two $\mathbb{Q}\mathbb{Z}_3$-modules
$M_1 := \mathbb{Q} \times \{0\}$. The element δ_1 acts as the identity on this module.
$M_2 := \{0\} \times \mathbb{Q}[x]/(x^2 + x + 1)$ The element δ_1 acts as $\overline{x}$ on this module.
The theory says that every $\mathbb{Q}\mathbb{Z}_3$-module is isomorphic to a direct sum $M_1^{(X)} \oplus M_2^{(Y)}$
Therefore there are two 'basic' representations in $\mathrm{Rep}_{\mathbb{Q}}(G)$ such that every other representation is equivalent to a direct sum of copies of these two.

Representations of $\mathbb{Z}_2$ over $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) \neq 2$

Maschke's theorem

Theorem

(Maschke) Let G be a finite group, $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$ a representation of G over $\mathbb{F}$, where $\mathbb{F}$ is a field such that $\mathrm{char}\,(\mathbb{F}) \nmid |G|$. If $U \leq V$ is a φ-invariant subspace of V, then there exists $W \leq V$ also φ-invariant such that $V = U \oplus W$. In particular, φ is equivalent to $\varphi_U \oplus \varphi_W$

Proof: For sure there is a vector space $W_0 \leq V$ such that $V = U \oplus W_0$.
But this space may not be φ-invariant so we have to modify it somehow.
Consider a homomorphism $\pi_0 \in \mathrm{End}_{\mathbb{F}}(V)$, a projection of V onto U with kernel W_0. That, is

$$\pi_0(u + w) := u; u \in U, w \in W_0$$

Averaging

(Important) We use 'averaging principle' to change π_0 to a linear map which is compatible with the action of G on V. This is how we do it:

$$\pi := \frac{1}{|G|} \sum_{g \in G} \varphi(g) \pi_0 \varphi(g^{-1}) \in \mathrm{End}_{\mathbb{F}}(V)$$

Note that here we needed $\mathrm{char}(\mathbb{F}) \nmid |G|$.

Outline of further steps

- $\pi \in \mathrm{Rep}_{\mathbb{F}}(V, V)$
- $\pi(u) = u$ for every $u \in U$, in particular $\pi \circ \pi = \pi$
- $\mathrm{Ker}\ \pi$ is a φ-invariant subspace
- $W := \mathrm{Ker}\ \pi$ satisfies $V = U \oplus W$

Compatibility with the action

We have to check that for every $g \in G$

$$\varphi(g) \circ \pi = \pi \circ \varphi(g)\,.$$

$$\varphi(g) \circ \pi = [\varphi(g)](\frac{1}{|G|} \sum_{h \in G} \varphi(h)\pi_0\varphi(h^{-1})) =$$

$$\frac{1}{|G|} \sum_{h \in G} \varphi(g)\varphi(h)\pi_0\varphi(h^{-1}(g^{-1}g))) =$$

$$\frac{1}{|G|} \sum_{h \in G} \varphi(gh)\pi_0\varphi((gh)^{-1}g) =$$

$$(\frac{1}{|G|} \sum_{h \in G} \varphi(h)\pi_0\varphi(h^{-1}))\varphi(g) =$$

$$\pi \circ \varphi(g)$$

$\pi \circ \pi = \pi$

Let $u \in U$. Writing φ_g instead of $\varphi(g)$ we get

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} \varphi_g(\pi_0(\varphi_{g^{-1}}(u))) = \frac{1}{|G|} \sum_{g \in G} \varphi_g(\varphi_{g^{-1}}(u))$$

(because $\varphi_{g^{-1}}(u) \in U$ and π_0 does not move elements of U)
Since $\varphi_g \circ \varphi_{g^{-1}} = 1_V$, $\varphi_{g^{-1}}(\varphi_g(u)) = u$.
So $\pi(u) = \frac{1}{|G|} \sum_{g \in G} u = u$.
Since $\mathrm{Im}\, \pi \subseteq U$, we get $\pi \circ \pi = \pi$.

$\mathrm{Ker}\ \pi$ is φ-invariant

It is a general fact that we will need later that if $\theta \in \mathrm{Rep}_{\mathbb{F}}(G)(\varphi_1, \varphi_2)$, then $\mathrm{Ker}\ \theta$ is a φ_1-invariant subspace and $\mathrm{Im}\ \theta$ is φ_2-invariant.
Let's do the particular case here:

$$W := \{v \in V \mid \pi(v) = 0\}$$

Let $g \in G$, $w \in W$ and again write φ_g instead of $\varphi(g)$:

$$\pi(\varphi_g(w)) = \varphi_g(\pi(w)) = \varphi_g(0) = 0$$

In other words $\varphi_g(w) \in W$ for every $g \in G$.
Therefore we proved W is indeed φ-invariant.

$V = U \oplus W$

$U \cap W = 0$: If $v \in U \cap W$ then

- $\pi(v) = v$ as π does not move elements of U
- $\pi(v) = 0$ by the definition of W

$U + W = V$: Take $v \in V$ put $v_U := \pi(v)$, $v_W := v - v_U$. Obviously $v = v_U + v_W$ and $v_U \in U$. Let us check that $v_W \in W$: $\pi(v_w) = \pi(v) - \pi(v_U) = \pi(v) - \pi(\pi(v)) = \pi(v) - \pi(v) = 0$. This completes the proof.

Thanks for your attention

Set of exercises on the averaging and the assumptions in the theorem of Maschke will be available tomorrow.