Group algebras, MARKUS M.R. TRIPP

→ development of modern noncommutative algebra was strongly motivated by <u>representation theory of groups</u>

IDEA OF REPRESENT. THEORY: study a group G by representing it in terms of linear transformations on a vector space V

Definition: A <u>representation of a group G</u> on a vector space V over a field K is a group homomorphism

$$\rho : G \to \mathrm{Aut}_K(V) := \{T : V \to V : T \text{ } K\text{-linear and invertible}\}$$

Remark: (1) This is equivalent to the existence of a "multiplication" $\cdot : G \times V \to V$ s.t.

$$g\cdot(h\cdot v) = (gh)\cdot v, \quad e\cdot v = v, \quad g\cdot(v+\lambda w) = g\cdot v + \lambda(g\cdot w)$$

for all $g, h \in G$, $\lambda \in K$, $v, w \in V$ (in short: a the linear structure of V preserving group action of G on V)

Proof: "⇒": Assume ρ representation; def. $\cdot : G\times V \to V$, $g\cdot v := \rho(g)(v)$

then: $g\cdot(h\cdot v) = \rho(g)(\underbrace{h\cdot v}_{=\rho(h)(v)}) = (\underbrace{\rho(g)\circ\rho(h)}_{=\rho(gh)})(v) = (gh)\cdot v$, ($\rho$ group hom!)

$e\cdot v = \underbrace{\rho(e)}_{=\mathrm{id}_V}(v) = v$ (ρ group hom!), $\quad g\cdot(v+\lambda w) = \rho(g)(v+\lambda w) \underset{\rho(g)\ K\text{-lin.}}{=} \rho(g)(v) + \lambda\rho(g)(w)$

$$= g\cdot v + \lambda(g\cdot w)$$

"⇐": Conversely, let $\cdot : G\times V \to V$ be a "multiplication"; def. $\rho : G \to \mathrm{Aut}_K(V)$ $\rho(g) := (v \mapsto g\cdot v)$ ring hom. □

In this situation, V is called a <u>G-module</u>.

(2) We can naturally transform V into an actual module over a ring; For this sake, we need to build G into a ring:

Definition: Let K be commutative ring (in most cases: K field), and G a group. The <u>group algebra</u> $K[G]$ is the free K-module with basis $g \in G$ and multiplication

$$\Big(\sum_{g\in G} a_g g\Big)\cdot\Big(\sum_{g\in G} b_g g\Big) := \sum_{g\in G}\Big(\sum_{\substack{g_1,g_2\in G:\\ g_1g_2=g}} a_{g_1} b_{g_2}\Big) g. \quad \leftarrow \text{convolution}$$

Remark: (1) It is routine verification that $K[G]$ is – as the terminology suggests – indeed a K-algebra.

- $\varepsilon : K \to K[G]$, $\lambda \mapsto \lambda(1_K e_G) = \lambda e_G$ (identity in $K[G]$) is a ring monomorphism, so we can regard K as a subring of $K[G]$ (identify λ with λe_G)
- $\iota : G \to K[G]$, $g \mapsto 1_K g$ is a group monomorphism, so we can regard G as a subgroup of $K[G]$ (identify g with $1_K g$)

⇝ so $K[G]$ is non-commutative unless the group G is commutative
$\big((1_K g)(1_K h) = (1_K h)(1_K g) \iff gh = hg\big)$

(2) Let G be a finite group; then $K[G]$ is <u>not</u> a division algebra.

Proof: let $g \in G\setminus\{e_G\}$, and $n = \mathrm{ord}(g) < \infty$ (as G finite) (smallest $k \in \mathbb{N}$ s.t. $g^k = e_G$)

then: $\underbrace{(1-g)}_{\neq 0}\underbrace{(1+g+\dots+g^{n-1})}_{\neq 0} = \sum_{i=0}^{n-1}(g^i - g^{i+1}) = 1 - \underbrace{g^n}_{=e_G} = 0$ □

(3) G can be relaxed to be a monoid – the construction still goes through.

(4) NOW: representations of G on vector spaces over a field K / G-modules $\overset{\text{one-to-one}}{\longleftrightarrow}$ $K[G]$-modules

If V is G-module, then $\left(\sum_{g\in G} a_g g\right)\cdot v := \sum_{g\in G} a_g (g\cdot v)$ makes V into a $K[G]$-mod.;
conversely, by restriction, every $K[G]$-module V is a G-module

(5) Let V, W be G-modules over K. We call a K-linear map $T: V\to W$
G-homomorphism if $T(g\cdot v) = g\cdot T(v)$ for all $g\in G$, $v\in V$.

THEN: besides the obvious changes in terminology,

$$G\text{-homomorphisms } V\to W \;\hat{=}\; K[G]\text{-module hom. } V\to W$$

If $T: V\to W$ G-hom., then $T\left(\left(\sum_{g\in G} a_g g\right)\cdot v\right) \overset{T\ K\text{-linear}}{=} \sum_{g\in G} a_g \underbrace{T(g\cdot v)}_{=g\cdot T(v)} =$

$\left(\sum_{g\in G} a_g g\right)\cdot v \overset{\text{Def.}}{=} \sum_{g\in G} a_g (g\cdot v)$

$\overset{\text{Def.}}{=} \left(\sum_{g\in G} a_g g\right)\cdot T(v)$;

conversely, by restriction, every $K[G]$-module hom $V\to W$ can be regarded as a G-homom.

(6) Similarly, for an K-algebra A, a monoid homomorphism $\varphi: G\to (A,\cdot)$ extends uniquely to an K-algebra homomorphism of $K[G]$ to A.

UNIQ.: any extension of φ would be in particular a K-module homom., so
$$\varphi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \varphi(g) \quad (*)$$

EXIST.: $(*)$ only candidate: K-module hom. ✓

▿ $\varphi\left(\underbrace{\left(\sum_{g_1\in G} a_{g_1} g_1\right)\left(\sum_{g_2\in G} b_{g_2} g_2\right)}_{=\sum_{g_1,g_2\in G} a_{g_1} b_{g_2} g_1 g_2}\right) = \sum_{g_1,g_2\in G} a_{g_1} b_{g_2} \underbrace{\varphi(g_1 g_2)}_{=\varphi(g_1)\varphi(g_2)} =$

$= \left(\sum_{g_1\in G} a_{g_1} g_1\right)\left(\sum_{g_2\in G} a_{g_2} g_2\right) = \varphi\left(\sum_{g_1\in G} a_{g_1} g_1\right)\varphi\left(\sum_{g_2\in G} b_{g_2} g_2\right)$

▿ $\varphi(1_K e_G) = 1_K \underbrace{\varphi(e_G)}_{=1_A} = 1_A$

Example: (1) if $G = (\mathbb{Z}, +)$, $K[G] \cong K[x, x^{-1}]$ (Laurent polynomials)

↑ element of form $\sum_{n \in \mathbb{Z}} a_n n \;\hat{=}\; \sum_{n \in \mathbb{Z}} a_n x^n$

Similarly, if $G = (\mathbb{N}_0^n, +)$, $K[G] \cong K[x_1, \dots, x_n]$ (Multivariate polynomials)

↑ element of form $\sum_{\alpha \in \mathbb{N}_0^n} a_\alpha \alpha \;\hat{=}\; \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha$

(2) Viewing $K[G]$ (← field) as a module over itself, gives rise to the so called <u>regular representation</u> of a group G.

e.g. $G = C_4 \rightsquigarrow K[C_4]$ as $K[C_4]$-module $\overset{\text{translates to}}{\longleftrightarrow}$ $K[C_4]$ as C_4-module

$= \{e_G, g, g^2, g^3\}$

$\longleftrightarrow$ representation ρ of C_4; $\rho : C_4 \to \mathrm{Aut}_K(K[C_4])$

$$\rho(g^i) = \Big(a_0 + a_1 g + a_2 g^2 + a_3 g^3 \longmapsto g^i (a_0 + a_1 g + a_2 g^2 + a_3 g^3)$$
$$= a_0 g^i + a_1 g^{i+1} + a_2 g^{i+2} + a_3 g^{i+3} \Big)$$

$\mathrm{Aut}_K(K[C_4]) \cong GL_4(K)$

$\longleftrightarrow$ def. $X : C_4 \to GL_4(K)$, $X(g^i) := [\rho(g^i)]_\alpha$ (representing matrix of $\rho(g^i)$ wrt basis α)

e.g. for g^2 and α std. basis of $K[C_4]$, we find

$$X(g^2) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

↑
$$\begin{cases} g^2 e_G = g^2 \\ g^2 g = g^3 \\ g^2 g^2 = e_G \\ g^2 g^3 = g \end{cases}$$

We call this a <u>matrix representation</u> (we can switch btw these notions if the module interpreted as a K-vector space is finite dimensional)

(3) let $G = S_n$ naturally act on $S := \{1, 2, \dots n\}$ (by permuting the elements of S)

extend action

→ then: $V = KS = \{a_1 1 + \ldots + a_n n : a_1, \ldots, a_n \in K\}$

with $\pi \cdot (a_1 1 + \ldots + a_n n) = a_1 \pi(1) + \ldots + a_n \pi(n)$ is S_n-module;

This is called the <u>defining representation</u> of S_n. As matrix represent. this reads as (wrt standard basis of KS)

$$X : S_n \to GL_n(K), \quad X(\pi) = (e_{\pi(j)})_{1 \leq j \leq n} \quad \leftarrow \text{permutation matrices}$$

$$\left((X(\pi))_{ij} = \begin{cases} 1 & \text{if } \pi(j) = i \\ 0 & \text{otherwise} \end{cases} \right)$$

Lastly, we present MASCHKE'S THEOREM – a main result regarding representations of a finite group G

→ for $K = \mathbb{C}$, it suffices to understand so-called irreducible representations of G / simple $K[G]$-modules as...

Theorem (Maschke): Let K be a field and G a finite group. Then, $K[G]$ is semisimple $\Leftrightarrow$ $\operatorname{char}(K) \nmid |G|$.

$\Updownarrow$ Th. 1.3.3 — every $K[G]$-module is semisimple

↑ $\operatorname{char}(K)$: smallest $n \in \mathbb{N}$ s.t. $n 1 = \underbrace{1 + \ldots + 1}_{n \text{ times}} = 0$ if such n exists, and 0 otherwise

Proof: "$\Leftarrow$": Let V be a $K[G]$-module

<u>We show:</u> every $K[G]$-submod. U of V is a direct summand $\Leftrightarrow$ ($\exists$ $K[G]$-submod. U' of V s.t. $V = U \oplus U'$)

$\underset{\text{Th. 1.2.4}}{\Leftrightarrow}$ V is semisimple

For this sake, let U be a $K[G]$-submodule of V; <u>IDEA</u>: construct projection $\pi : V \to V$ onto U that is a also a $K[G]$-module homomorphism

$$\Rightarrow \quad V = \underbrace{\operatorname{im} \pi}_{= U} \oplus \underbrace{\ker \pi}_{= U'}, \quad U' \ K[G]\text{-submodule}$$

↑ projection means $\pi^2 = \pi$;

let $v \in V$, then $v = \underbrace{\pi(v)}_{\in \operatorname{im} \pi} + \underbrace{(v - \pi(v))}_{\in \ker \pi} \Rightarrow V = U + U'$ (since: $\pi(v - \pi(v)) = \pi(v) - \pi^2(v) = 0$)

let $w \in \operatorname{im} \pi \cap \ker \pi$, then: $w = \pi(v) = \pi(\underbrace{\pi(v)}_{= 0}) = 0 \Rightarrow V = U \oplus U'$

$\Rightarrow w = \pi(v)$ for some $v \in V$

let $\pi_0 : V \to V$ be any K-linear map such that $\pi_0^2 = \pi_0$ and $\operatorname{im} \pi_0 = U$
(to construct it, choose a basis for U and extend it to a basis of V, set $\pi_0|_U = \mathrm{id}_U$ and do whatever you like on the other basis vectors as long as images lie in U; $\pi^2(v) = \pi(\underbrace{\pi(v)}_{\in U}) = \pi(v)$, $\forall v \in V$) $\pi|_U = \mathrm{id}_U$

turn π_0 in a $\rightsquigarrow$ K[G]-module hom.

$$\pi : V \to V, \quad \pi(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi_0(gv)$$

$\frac{1}{|G|} = (\underbrace{|G| \cdot 1}_{= 1 + \ldots + 1 \neq 0})^{-1}$ exists (because $\operatorname{char}(K) \nmid |G|$)

<u>CLAIM 1</u>: π K[G]-module homomorphism ($\Leftrightarrow$ π is a G-module hom.)

- π still K-linear as $v, w \in V, \lambda \in K$:

$$\pi(v + \lambda w) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi_0(\underbrace{g(v + \lambda w)}_{= gv + \lambda(gw)}) =$$

π_0 K-lin.

$$= \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi_0(gv) + \lambda \left(\frac{1}{|G|} \sum_{g \in G} g^{-1} \pi_0(gw) \right) = \pi(v) + \lambda \pi(w)$$

- let $v \in V, h \in G$; $\pi(hv) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi_0(\underbrace{g(hv)}_{= (gh)v}) =$

$$= \underbrace{h h^{-1}}_{= e_G} \sum_{g \in G} g^{-1} \pi_0((gh)v) = h \sum_{g \in G} \underbrace{h^{-1} g^{-1}}_{= (gh)^{-1}} \pi_0((gh)v) = h \sum_{k \in G} k^{-1} \pi_0(kv) = h\pi(v)$$

($g \mapsto gh$ bijective)

<u>CLAIM 2</u>: π projection with $\operatorname{im} \pi = U$

note, $\operatorname{im} \pi \subseteq U$ as $\forall v \in V, \forall g \in G$: $\pi_0(\underbrace{gv}_{\in V}) \in U \Rightarrow$

U K[G]-mod.

$$\Rightarrow \quad \pi(v) = \frac{1}{|G|} \sum_{g \in G} \underbrace{g^{-1} \pi(gv)}_{\in U} \in U;$$

remains to show, $\pi|_U \overset{!}{=} \mathrm{id}_U$: let $u \in U$, $\pi(u) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \underbrace{\pi_0(\underset{\in U}{gu})}_{= gu} = \frac{1}{|G|} \sum_{g \in G} u = u$

"$\Rightarrow$": by contrapositive, assume $\mathrm{char}(K) \mid |G|$; By Th. 1.4.10, it suffices to show $J(K[G]) \neq 0$ ($\Rightarrow K[G]$ not semisimple)

R semisimple $\Leftrightarrow$
$\Leftrightarrow$ R Artinian and $J(R) = 0$

def. $e := \sum_{g \in G} g \in K[G] \setminus \{0\}$

observe that $\forall h \in G$, $he = \sum_{g \in G} \underbrace{hg}_{=: k \in G} = \sum_{k \in G} k = e$, thus:

$$e^2 = \underbrace{\left(\sum_{g \in G} g\right)}_{= e} \cdot e = \sum_{g \in G} \underbrace{ge}_{= e} \underset{\mathrm{char}(K) \mid |G|}{\overset{\uparrow}{=}} 0 ;$$

$K[G]e \underset{\forall h \in G,\, he = e}{=} Ke$ nil left ideal $\overset{L. 1.4.6(2)}{\Rightarrow} K[G]e \subseteq J(K[G])$, so that $J(K[G]) \neq 0$

□