Algebra, Chapter 0

By Paolo Aluffi

2.1 One can associate an $n \times n$ matrix M_{σ} with a permutation $\sigma \in S_n$, by letting the entry at $(i, \sigma(i))$ be 1, and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

would be

$$M_{\sigma} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Prove that, with this notation,

$$M_{\sigma\tau} = M_{\sigma}M_{\tau}$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices.

With Kronecker delta function

$$\delta_{i,j} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j, \end{cases}$$

the entry at (i,j) of the matrix $M_{\sigma\tau}$ can be written as

$$(M_{\sigma\tau})_{i,j} = \delta_{\tau(\sigma(i)),j}$$

and the entry at (i,j) of the matrix $M_{\sigma}M_{\tau}$ can be written as

$$(M_{\sigma}M_{\tau})_{i,j} = \sum_{k=1}^{n} (M_{\sigma})_{i,k} (M_{\tau})_{k,j} = \sum_{k=1}^{n} \delta_{\sigma(i),k} \cdot \delta_{\tau(k),j} = \sum_{k=1}^{n} \delta_{\sigma(i),k} \cdot \delta_{k,\tau^{-1}(j)} = \delta_{\sigma(i),\tau^{-1}(j)}.$$

Note that

$$\tau(\sigma(i)) = j \iff \sigma(i) = \tau^{-1}(j).$$

we see $M_{\sigma\tau} = M_{\sigma}M_{\tau}$ for all $\sigma, \tau \in S_n$.

2.2 Prove that if $d \leq n$, then S_n contains elements of order d.

The cyclic permutation

$$\sigma = (1 \ 2 \ 3 \cdots d)$$

is an element of order d in S_n .

2.3 For every positive integer n find an element of order n in $S_{\mathbb{N}}$.

The cyclic permutation

$$\sigma = (1 \ 2 \ 3 \cdots n)$$

is an element of order d in S_n .

2.4 Define a homomorphism $D_8 \to S_4$ by labeling vertices of a square, as we did for a triangle in §2.2. List the 8 permutations in the image of this homomorphism.

The image of n rotations under the homomorphism are

$$\sigma_1 = e_{D_8}, \ \sigma_2 = (1\ 2\ 3\ 4), \ \sigma_3 = (1\ 3)(2\ 4), \ \sigma_4 = (1\ 4\ 3\ 2).$$

The image of n reflections under the homomorphism are

$$\sigma_5 = (1\ 3), \ \sigma_6 = (2\ 4), \ \sigma_7 = (1\ 2)(3\ 4), \ \sigma_8 = (1\ 4)(3\ 2).$$

3.1 Let $\varphi:G\to H$ be a morphism in a category C with products. Explain why there is a unique morphism

$$(\varphi \times \varphi): G \times G \longrightarrow H \times H.$$

(This morphism is defined explicitly for C = Set in §3.1.)

By the universal property of product in C, there exist a unique morphism $(\varphi \times \varphi) : G \times G \longrightarrow H \times H$ such that the following diagram commutes.

$$G \xrightarrow{\varphi} H$$

$$\uparrow^{\pi_G} \qquad \uparrow^{\pi_H}$$

$$G \times G \xrightarrow{\varphi \times \varphi} H \times H$$

$$\uparrow^{\pi_G} \qquad \downarrow^{\pi_H}$$

$$G \xrightarrow{\varphi} H$$

2

3.2 Let $\varphi: G \to H, \psi: H \to K$ be morphisms in a category with products, and consider morphisms between the products $G \times G, H \times H, K \times K$ as in Exercise 3.1. Prove that

$$(\psi\varphi)\times(\psi\varphi)=(\psi\times\psi)(\varphi\times\varphi).$$

(This is part of the commutativity of the diagram displayed in §3.2.)

By the universal property of product in C, there exist a unique morphism

$$(\psi\varphi)\times(\psi\varphi):G\times G\to K\times K$$

such that the following diagram commutes.

$$G \xrightarrow{\psi\varphi} H$$

$$\pi_{G} \downarrow \qquad \qquad \uparrow \pi_{H}$$

$$G \times G \xrightarrow{(\psi\varphi)\times(\psi\varphi)} H \times H$$

$$\pi_{G} \downarrow \qquad \qquad \downarrow \pi_{H}$$

$$G \xrightarrow{\psi\varphi} H$$

As the following commuting diagram tells us the composition

$$(\psi \times \psi)(\varphi \times \varphi) : G \times G \to K \times K$$

can make the above diagram commute,

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K$$

$$\pi_{G} \downarrow \qquad \pi_{H} \downarrow \qquad \pi_{K} \downarrow$$

$$G \times G \xrightarrow{\varphi \times \varphi} H \times H \xrightarrow{\psi \times \psi} K \times K$$

$$\pi_{G} \downarrow \qquad \pi_{H} \downarrow \qquad \pi_{K} \downarrow$$

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K$$

there must be $(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi)$.

3.3 Show that if G, H are abelian groups, then $G \times H$ satisfies the universal property for coproducts in Ab .

Define two monomorphisms:

$$i_G: G \longrightarrow G \times H, \ a \longmapsto (a, 0_H)$$

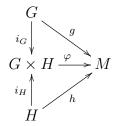
$$i_H: H \longrightarrow G \times H, \ b \longmapsto (0_G, b)$$

We are proving that for any two homomorphisms $g: G \to M$ and $h: H \to M$ in Ab, the map

$$\varphi: G \times H \longrightarrow M,$$

 $(a,b) \longmapsto q(a) + h(b)$

is a homomorphism and makes the following diagram commute.



Exploiting the fact that g, h are homomorphisms and M is an abelian group, it is easy to check that φ preserves the addition operation

$$\varphi((a_1, b_1) + (a_2, b_2)) = \varphi((a_1 + a_2, b_1 + b_2))$$

$$= g(a_1 + a_2) + h(b_1 + b_2)$$

$$= (g(a_1) + g(a_2)) + (h(b_1) + h(b_2))$$

$$= (g(a_1) + h(b_1)) + (g(a_2) + h(b_2))$$

$$= g(a_1 + b_1) + h(a_2 + b_2)$$

$$= \varphi((a_1, b_1)) + \varphi((a_2, b_2))$$

and the diagram commutes

$$\varphi \circ i_G(a) = \varphi((a, 0_H)) = g(a) + h(0_H) = g(a) + 0_M = g(a),$$

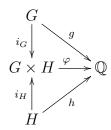
$$\varphi \circ i_H(b) = \varphi((0_G, b)) = g(0_G) + h(b) = 0_M + h(b) = h(b).$$

To show the uniqueness of the homomorphism φ we have constructed, suppose a homomorphism φ' can make the diagram commute. Then we have

$$\varphi'((a,b)) = \varphi'((a,0_H) + (0_G,b)) = \varphi'(i_G(a)) + \varphi'(i_H(b)) = g(a) + h(b) = \varphi((a,b)),$$

that is $\varphi' = \varphi$. Hence we show that there exist a unique homomorphism φ such that the diagram commutes, which amounts to the universal property for coproducts in Ab.

3.3 Prove that \mathbb{Q} is not the direct product of two nontrivial groups.



Consider the additive group of rationals $(\mathbb{Q}, +)$. Assume the product $G \times H = \{(a, b) | a \in G, b \in H\}$ is isomorphic to $(\mathbb{Q}, +)$. Note that $\{e_G\} \times H$ and $G \times \{e_H\}$ are subgroups in $G \times H$ and there intersection is trivial group $\{e_G\} \times \{e_H\}$. The commutative diagram implies

$$\varphi(\lbrace e_G\rbrace \times H) = \varphi(i_H(H)) = h(H),$$

$$\varphi(G \times \{e_H\}) = \varphi(i_G(G)) = g(G).$$

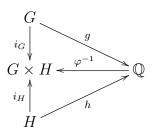
It is easy to check bijection φ satisfies $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$. Hence we have

$$\varphi(\{(e_G, e_H)\}) = \varphi(\{e_G\} \times H \cap G \times \{e_H\}) = \varphi(\{e_G\} \times H) \cap \varphi(G \times \{e_H\}) = h(H) \cap g(G) = \{0\}.$$

Suppose both g(G) and h(H) are nontrivial groups. If $\frac{p}{q} \in h(H) - \{0\}$ and $\frac{r}{s} \in g(G) - \{0\}$, there must be

$$rp = rq \cdot \frac{p}{q} = ps \cdot \frac{r}{s} \in h(H) \cap g(G).$$

Since $rp \neq 0$, it leads to a contradiction. Thus we can assume g(G) is a trivial group. According to the dual commutative diagram,



we see that for all $a \in G$,

$$(a, e_H) = i_(a) = \varphi^{-1}(g(a)) = \varphi(0) = (e_G, e_H) \implies a = e_G.$$

that is, G is a trivial group. Therefore, we have shown $(\mathbb{Q}, +)$ will never be isomorphic to the direct product of two nontrivial groups.

Assume

$$\varphi(a_1, b_1) = g(a_1) + h(b_1) = 1,$$

By induction we can show for all $p \in \mathbb{N}$.

$$\varphi(a_1^p, b_1^p) = pg(a_1) + ph(b_1) = p,$$

For all $q \in \mathbb{N} - \{0\}$, there exist unique $(c_q, d_q) \in G \times H$ such that

$$\varphi(c_q, d_q) = g(c_q) + h(d_q) = \frac{1}{q},$$

namely

$$\varphi(c_q^q, d_q^q) = q\varphi(c_q, d_q) = 1 = \varphi(a_1, b_1) \implies (c_q^q, d_q^q) = (a_1, b_1).$$

Denote $c_q = a_1^{\frac{1}{q}}, \ d_q = b_1^{\frac{1}{q}}.$

$$\varphi([(a_1^{\frac{1}{q}})^p]^q,[(b_1^{\frac{1}{q}})^p]^q)=\varphi((a_1^{\frac{1}{q}})^{pq},(b_1^{\frac{1}{q}})^{pq})=pq\varphi((a_1^{\frac{1}{q}},b_1^{\frac{1}{q}}))=pq\frac{1}{q}=\varphi(a_1^p,b_1^p)$$

implies

$$[(a_1^{\frac{1}{q}})^p]^q = a_1^p, \ [(b_1^{\frac{1}{q}})^p]^q = b_1^p$$

Denote $(a_1^{\frac{1}{q}})^p = (a_1^p)^{\frac{1}{q}} = a_1^{\frac{p}{q}}, \ (b_1^{\frac{1}{q}})^p = (b_1^p)^{\frac{1}{q}} = b_1^{\frac{p}{q}}.$ Then

$$g(a_1^{\frac{p}{q}}) = pg(a_1^{\frac{1}{q}}) = \frac{p}{q}g(a_1)$$

$$h(b_1^{\frac{p}{q}}) = ph(b_1^{\frac{1}{q}}) = \frac{p}{q}h(b_1).$$

For all $p \in \mathbb{N}$, if $h(b_1) \neq 0$,

$$p = \varphi(a_1^p, b_1^p)$$

$$= (p+1)g(a_1) + \left(p - \frac{g(a_1)}{h(b_1)}\right)h(b_1)$$

$$= g(a_1^{p+1}) + h\left(b_1^{p - \frac{g(a_1)}{h(b_1)}}\right)$$

$$= \varphi\left(a_1^{p+1}, b_1^{p - \frac{g(a_1)}{h(b_1)}}\right)$$

Therefore, $a_1^p = a_1^{p+1} \implies a_1 = e_G$ Hence for all $\frac{p}{q} \in \mathbb{Q}$, it holds that

$$\frac{p}{q} = p\varphi(a_1^{\frac{1}{q}}, b_1^{\frac{1}{q}}) = \varphi(a_1^{\frac{p}{q}}, b_1^{\frac{p}{q}}) = \frac{p}{q}g(a_1) + \frac{p}{q}h(b_1).$$

Suppose

$$\varphi(a_1, e_H) = \frac{r}{s} = \varphi(c_s^r, d_s^r),$$

which indicates

$$(a_1, e_H) = (c_s^r, d_s^r) \implies d_s^r = e_H.$$

Likewise, we suppose

$$\varphi(e_G, d_q^p) = \frac{m}{n} = \varphi(c_n^m, d_n^m),$$

and get $c_n^m = e_G$.

$$\varphi(c_q^p, d_q^p) = \varphi(c_q^p, e_H) + \varphi(e_G, d_q^p) = rg(c_s) + mh(d_n)$$