Huyi Chen

2018/03/31

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

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

∎

2.11 Prove that the square of every odd integer is congruent to 1 modulo 8.

Given an odd integer $2k+1$, we have

$$(2k+1)^2 = 4k(k+1) + 1,$$

where $k(k+1)$ is an even integer. So $(2k+1)^2 \equiv 1 \mod 8$. ∎

2.12 Prove that there are no integers a, b, c such that $a^2 + b^2 = 3c^2$. (Hint: studying the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$, show that a, b, c would all have to be even. Letting $a = 2k, b = 2l, c = 2m$, you would have $k^2 + l^2 = 3m^2$. What's wrong with that?)

$$a^2 + b^2 = 3c^2 \implies [a]_4^2 + [b]_4^2 = 3[c]_4^2.$$

Noting that $[0]_4^2 = [0]_4, [1]_4^2 = [1]_4, [2]_4^2 = [0]_4, [3]_4^2 = [1]_4$, we see $[c]_4^2$ must be $[0]_4$ and so do $[a]_4^2$ and $[b]_4^2$. Hence $[a]_4, [b]_4, [b]_4$ can only be $[0]_4$ or $[2]_4$, which justifies letting $a = 2k_1, b = 2l_2, c = 2m_1$. After substitution we have $k^2 + l^2 = 3m^2$. Repeating this process n times yields $a = 2^n k_n, b = 2^n l_n, c = 2^n m_n$. For a sufficiently large number N, the absolute value of k_N, l_N, m_N must be less than 1. Thus we conclude that $a = b = c = 0$ is the unique solution to the equation $a^2 + b^2 = 3c^2$. ■

2.13 Prove that if $\gcd(m, n) = 1$, then there exist integers a and b such that $am + bn = 1$. (Use Corollary 2.5.) Conversely, prove that if $am + bn = 1$ for some integers a and b, then $\gcd(m, n) = 1$. [2.15, §V.2.1, V.2.4]

Applying corollary 2.5, we have $\gcd(m, n) = 1$ if and only if $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. Hence

$$\gcd(m, n) = 1 \iff a[m]_n = [1]_n \iff [am]_n = [1]_n \iff am + bn = 1.$$

■

2.15 Let $n > 0$ be an odd integer.

- Prove that if $\gcd(m, n) = 1$, then $\gcd(2m + n, 2n) = 1$. (Use Exercise 2.13.)
- Prove that if $\gcd(r, 2n) = 1$, then $\gcd(\frac{r+n}{2}, n) = 1$. (Ditto.)
- Conclude that the function $[m]_n \to [2m + n]_{2n}$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

The number $\phi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is Eulers $\phi(n)$-function. The reader has just proved that if n is odd, then $\phi(2n) = \phi(n)$. Much more general formulas will be given later on (cf. Exercise V.6.8). [VII.5.11]

- According to 2.13,

  $$\gcd(m, n) = 1 \implies am + bn = 1 \implies \frac{a}{2}(2m + n) + \left(b - \frac{a}{2}\right) n = 1.$$

  If a is even, we have shown $\gcd(2m + n, 2n) = 1$. Otherwise we can let $a' = a + n$ be an even integer and $b' = b - m$. Then it holds that

  $$\frac{a'}{2}(2m + n) + \left(b' - \frac{a'}{2}\right) n = 1,$$

which also indicates $\gcd(2m+n, 2n) = 1$.

- If $\gcd(r, 2n) = 1$, then r must be an odd integer and accordingly

$$\gcd(2r+2n, 4n) = 1 \implies a(2r+2n) + b(4n) = 1 \implies 4a\frac{r+n}{2} + 4bn = 1,$$

which is $\gcd(\frac{r+n}{2}, n) = 1$.

- It is easy to check that the function $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*,\ [m]_n \mapsto [2m+n]_{2n}$ is well-defined. The fact

$$\begin{aligned} f([m_1]_n) = f([m_2]_n) &\implies f([2m_1+n]_{2n}) = f([2m_2+n]_{2n}) \\ &\implies (2m_1+n) - (2m_2+n) = 2kn \\ &\implies m_1 - m_2 = kn \\ &\implies [m_1]_n = [m_2]_n \end{aligned}$$

indicates that f is injective. For any $[r]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$, we have

$$\gcd(r, 2n) = 1 \implies \gcd\left(\frac{r+n}{2}, n\right) = 1 \implies \left[\frac{r+n}{2}\right]_n \in (\mathbb{Z}/n\mathbb{Z})^*,$$

and

$$f\left(\left[\frac{r+n}{2}\right]_n\right) = [r+2n]_{2n} = [r]_{2n},$$

which indicates that f is surjective.

■

> **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 $\mathsf{C} = \mathsf{Set}$ 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.

$$\begin{tikzcd} G \arrow[r, "\varphi"] & H \\ G \times G \arrow[u, "\pi_G"] \arrow[r, "\varphi\times\varphi"] \arrow[d, "\pi_G"'] & H \times H \arrow[u, "\pi_H"'] \arrow[d, "\pi_H"] \\ G \arrow[r, "\varphi"] & H \end{tikzcd}$$

■

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.

$$\begin{tikzcd}
G \arrow[r, "\psi\varphi"] & H \\
G \times G \arrow[u, "\pi_G"] \arrow[d, "\pi_G"'] \arrow[r, "(\psi\varphi)\times(\psi\varphi)"] & H \times H \arrow[u, "\pi_H"'] \arrow[d, "\pi_H"] \\
G \arrow[r, "\psi\varphi"] & H
\end{tikzcd}$$

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,

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[rr, bend left, "\psi\varphi"] & H \arrow[r, "\psi"] & K \\
G \times G \arrow[u, "\pi_G"] \arrow[d, "\pi_G"'] \arrow[r, "\varphi\times\varphi"] & H \times H \arrow[u, "\pi_H"] \arrow[d, "\pi_H"'] \arrow[r, "\psi\times\psi"] & K \times K \arrow[u, "\pi_K"] \arrow[d, "\pi_K"'] \\
G \arrow[r, "\varphi"] \arrow[rr, bend right, "\psi\varphi"'] & H \arrow[r, "\psi"] & K
\end{tikzcd}$$

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

$$\begin{aligned} \varphi : \quad & G \times H \longrightarrow M, \\ & (a, b) \longmapsto g(a) + h(b) \end{aligned}$$

is a homomorphism and makes the following diagram commute.

$$\begin{tikzcd} G \arrow[d, "i_G"'] \arrow[dr, "g"] & \\ G \times H \arrow[r, "\varphi"] & M \\ H \arrow[u, "i_H"] \arrow[ur, "h"'] & \end{tikzcd}$$

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

$$\begin{aligned} \varphi((a_1, b_1) + (a_2, b_2)) &= \varphi((a_1 + a_2, b_1 + b_2)) \\ &= g(a_1 + a_2) + h(b_1 + b_2) \\ &= (g(a_1) + g(a_2)) + (h(b_1) + h(b_2)) \\ &= (g(a_1) + h(b_1)) + (g(a_2) + h(b_2)) \\ &= g(a_1 + b_1) + h(a_2 + b_2) \\ &= \varphi((a_1, b_1)) + \varphi((a_2, b_2)) \end{aligned}$$

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.

$$\begin{tikzcd}
G \arrow[d, "i_G"'] \arrow[dr, "g"] & \\
G \times H \arrow[r, "\varphi"] & \mathbb{Q} \\
H \arrow[u, "i_H"] \arrow[ur, "h"'] &
\end{tikzcd}$$

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

$$\varphi(\{e_G\} \times H) = \varphi(i_H(H)) = h(H),$$

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

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 $\dfrac{p}{q} \in h(H) - \{0\}$ and $\dfrac{r}{s} \in g(G) - \{0\}$, 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,

$$\begin{tikzcd}
G \arrow[d, "i_G"'] \arrow[dr, "g"] & \\
G \times H & \mathbb{Q} \arrow[l, "\varphi^{-1}"'] \\
H \arrow[u, "i_H"] \arrow[ur, "h"'] &
\end{tikzcd}$$

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. ∎