Huyi Chen

2018/03/31

Algebra, Chapter 0

By Paolo Aluffi

Contents

Chapter I. Preliminaries: Set theory and categories

§1. Naive Set Theory

1.6 Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers, by setting $a \sim b \iff b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for $\mathbb{R}/\sim$. Do the same for the relation $\approx$ on the plane $\mathbb{R} \times \mathbb{R}$ defined by declaring $(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$. [§II.8.1, II.8.10]

Imaginatively, $\mathbb{R}/\sim$ can be viewed as a ring of length 1 by bending the real line $\mathbb{R}$. Then we can rotate a ring around an axis of rotation to get $\mathbb{R} \times \mathbb{R}/\approx$, which makes a torus. ∎

§2. Functions between sets

2.1 How many different bijections are there between a set S with n elements and itself? [§II.2.1]

There are $n!$ different bijections $S \to S$. ∎

§3. Categories

3.1 Let C be a category. Consider a structure C^{op} with:

- $\mathrm{Obj}(\mathsf{C}^{op}) := \mathrm{Obj}(\mathsf{C})$;
- for A, B objects of C^{op} (hence, objects of C), $\mathrm{Hom}_{\mathsf{C}^{op}}(A, B) := \mathrm{Hom}_{\mathsf{C}}(B, A)$

Show how to make this into a category (that is, define composition of morphisms in C^{op} and verify the properties listed in §3.1). Intuitively, the 'opposite' category C^{op} is simply obtained by 'reversing all the arrows' in C. [5.1, §VIII.1.1, §IX.1.2, IX.1.10]

- For every object A of C, there exists one identity morphism $1_A \in \mathrm{Hom}_{\mathsf{C}}(A, A)$. Since $\mathrm{Obj}(\mathsf{C}^{op}) := \mathrm{Obj}(\mathsf{C})$ and $\mathrm{Hom}_{\mathsf{C}^{op}}(A, A) := \mathrm{Hom}_{\mathsf{C}}(A, A)$, for every object A of C^{op}, the identity on A coincides with $1_A \in \mathsf{C}$.
- For A, B, C objects of C^{op} and $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B) = \mathrm{Hom}_{\mathsf{C}}(B, A)$, $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C) = \mathrm{Hom}_{\mathsf{C}}(C, B)$, the composition laws in C determines a morphism $f * g$ in $\mathrm{Hom}_{\mathsf{C}}(C, A)$, which deduces the composition defined on C^{op}:

$$\begin{aligned} \mathrm{Hom}_{\mathsf{C}^{op}}(A, B) \times \mathrm{Hom}_{\mathsf{C}^{op}}(B, C) &\longrightarrow \mathrm{Hom}_{\mathsf{C}^{op}}(A, C) \\ (f, g) &\longmapsto g \circ f := f * g \end{aligned}$$

- Associativity. If $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$, $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C)$, $h \in \mathrm{Hom}_{\mathsf{C}^{op}}(C, D)$, then

$$f \circ (g \circ h) = f \circ (h * g) = (h * g) * f = h * (g * f) = (g * f) \circ h = (f \circ g) \circ h.$$

- Identity. For all $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$, we have

$$f \circ 1_A = 1_A * f = f, \quad 1_B \circ f = f * 1_B = f.$$

Thus we get the full construction of C^{op}. ∎

§4. Morphisms

4.2 In Example 3.3 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid (cf. Example 4.6)? [§4.1]

For a reflexive and transitive relation $\sim$ on a set S, define the category C as follows:

- Objects: $\mathrm{Obj}(\mathsf{C}) = S$;

- Morphisms: if a, b are objects (that is: if $a, b \in S$) then let

$$\mathrm{Hom}_{\mathsf{C}}(a,b) = \begin{cases} (a,b) \in S \times S & \text{if } a \sim b \\ \emptyset & \text{otherwise} \end{cases}$$

In Example 3.3 we have shown the category. If the relation $\sim$ is endowed with symmetry, we have

$$(a,b) \in \mathrm{Hom}_{\mathsf{C}}(a,b) \implies a \sim b \implies b \sim a \implies (b,a) \in \mathrm{Hom}_{\mathsf{C}}(b,a).$$

Since

$$(a,b)(b,a) = (a,a) = 1_a, \quad (b,a)(a,b) = (b,b) = 1_b,$$

in fact (a,b) is an isomorphism. From the arbitrariness of the choice of (a,b), we show that C is a groupoid. Conversely, if C is a groupoid, we can show the relation $\sim$ is symmetric. To sum up, the category C is a groupoid if and only if the corresponding relation $\sim$ is an equivalence relation. ∎

§5. Universal properties

5.1 Prove that a final object in a category C is initial in the opposite category C_{op} (cf. Exercise 3.1).

An object F of C is final in C if and only if

$$\forall A \in \mathrm{Obj}(\mathsf{C}) : \mathrm{Hom}_{\mathsf{C}}(A,F) \text{ is a singleton.}$$

That is equivalent to

$$\forall A \in \mathrm{Obj}(\mathsf{C}_{op}) : \mathrm{Hom}_{\mathsf{C}_{op}}(F,A) \text{ is a singleton,}$$

which means F is initial in the opposite category C_{op}. ∎

Chapter II. Groups, first encounter

§1. Definition of group

1.1 Write a careful proof that every group is the group of isomorphisms of a groupoid. In particular, every group is the group of automorphisms of some object in some category.

Assume G is a group. Define a category C as follows:

- Objects: $\mathrm{Obj}(\mathsf{C}) = \{*\}$;

- Morphisms: $\mathrm{Hom}_{\mathsf{C}}(*,*) = \mathrm{End}_{\mathsf{C}}(*) = G$.

The composition of homomorphism is corresponding to the multiplication between two elements in G. The identity morphism on $*$ is $1_* = e_G$, which satisfies for all $g \in \mathrm{Hom}_{\mathsf{C}}(*,*)$,

$$ge_G = e_G g = g,$$

and

$$gg^{-1} = e_G,\ g^{-1}g = e_G.$$

Thus any homomorphism $g \in \mathrm{Hom}_{\mathsf{C}}(*,*)$ is an isomorphism and accordingly C is a groupoid. Now we see $G = \mathrm{End}_{\mathsf{C}}(*)$ is the group of isomorphisms of a groupoid. Moreover, supposing that $*$ is an object in some category D, G would be the group of automorphisms of $*$, which is denoted as $\mathrm{Aut}_{\mathsf{D}}(*)$. ∎

1.4 Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

For all $a, b \in G$,

$$abab = e \implies a(abab)b = ab \implies (aa)ba(bb) = ab \implies ba = ab.$$

∎

§2. Examples of groups

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.

By introducing the 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

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

where the last but one equality holds by the fact

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

Noticing 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 Exercise 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. Thus we show f is a bijection.

■

2.16 Find the last digit of $1238237^{18238456}$. (Work in $\mathbb{Z}/10\mathbb{Z}$.)

$$1238237^{18238456} \equiv 7^{18238456} \equiv (7^4)^{4559614} \equiv 2401^{4559614} \equiv 1 \mod 10,$$

which indicates that the last digit of $1238237^{18238456}$ is 1. ■

2.17 Show that if $m \equiv m' \mod n$, then $\gcd(m, n) = 1$ if and only if $\gcd(m', n) = 1$. [§2.3]

Assume that $m - m' = kn$. If $\gcd(m, n) = 1$, for any common divisor d of m' and n

$$d|m',\ d|n \implies d|(m'+kn) \implies d|m \implies d = 1,$$

which means $\gcd(m', n) = 1$. Likewise, we can show $\gcd(m', n) = 1 \implies \gcd(m, n) = 1$ ■

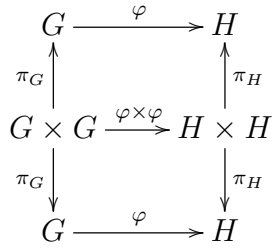
§3. The category Grp

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.



■

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

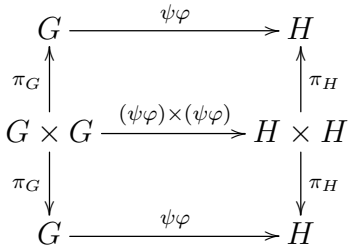
$$(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi).$$

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

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

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

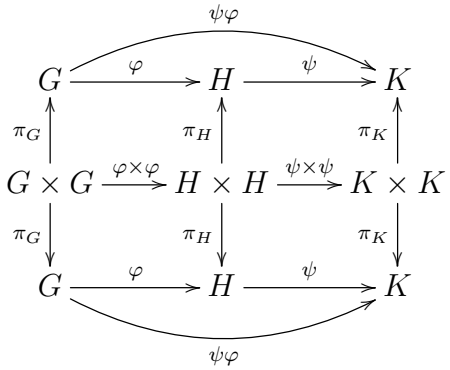
such that the following diagram commutes.



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,



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:

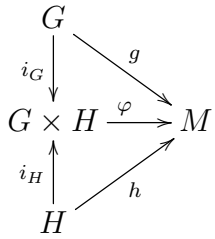
$$i_G : G \longrightarrow G \times H,\ a \longmapsto (a, 0_H)$$

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

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

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

is a homomorphism and makes the following diagram commute.



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.

∎

3.4 Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial? (Hint: No. Can you construct a counterexample?)

Consider the function

$$\begin{aligned}\varphi : \mathbb{Z}\times\mathbb{Z}[x] &\longrightarrow \mathbb{Z}[x]\\ (n, f(x)) &\longmapsto n + xf(x)\end{aligned}$$

Firstly, we can show φ is a homomorphism as follows

$$\begin{aligned}\varphi((n_1,f_1(x))+(n_2,f_2(x))) &= \varphi((n_1+n_2,f_1(x)+f_2(x)))\\ &= (n_1+n_2)+x(f_1(x)+f_2(x))\\ &= (n_1+xf_1(x))+(n_2+xf_2(x))\\ &= \varphi((n_1,f_1(x)))+\varphi((n_2,f_2(x))).\end{aligned}$$

Secondly, we are to show φ is a monomorphism. It follows by

$$\varphi((n,f(x)))=n+xf(x)=0 \implies n=0,\ f(x)=0 \implies \ker\varphi=\{(0,0)\}.$$

Lastly, since the cardinal numbers of both $\mathbb{Z}\times\mathbb{Z}[x]$ and $\mathbb{Z}[x]$ are $\aleph_0$, φ is indeed an isomorphism. Therefore, as a counterexample we have $\mathbb{Z}[x]\cong\mathbb{Z}\times\mathbb{Z}[x]$. ∎

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

Consider the additive group of rationals $(\mathbb{Q}, +)$. Assume that φ is a isomorphism between the product $G \times H = \{(a, b) | a \in G, b \in H\}$ and $(\mathbb{Q}, +)$. Note that $\{e_G\} \times H$ and $G \times \{e_H\}$ are subgroups in $G \times H$ and their intersection is the trivial group $\{(e_G, e_H)\}$. It is easy to check that bijection φ satisfies $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$. So applying the fact we have

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

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

$$rp = rq \cdot \frac{p}{q} = ps \cdot \frac{r}{s} \in \varphi(\{e_G\} \times H) \cap \varphi(G \times \{e_H\}),$$

which implies $rp = 0$. Since both $\frac{p}{q}$ and $\frac{r}{s}$ are non-zero, it leads to a contradiction. Thus without loss of generality we can assume $\varphi(\{e_G\} \times H)$ is a trivial group $\{0\}$. Since φ is isomorphism, we see that for all $h \in H$,

$$\varphi(e_G, h) = \varphi(e_G, e_H) = 0 \iff h = e_H.$$

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

3.6 Consider the product of the cyclic groups C_2, C_3 (cf. §2.3): $C_2 \times C_3$. By Exercise 3.3, this group is a coproduct of C_2 and C_3 in Ab. Show that it is not a coproduct of C_2 and C_3 in Grp, as follows:

- find injective homomorphisms $C_2 \to S_3$, $C_3 \to S_3$;
- arguing by contradiction, assume that $C_2 \times C_3$ is a coproduct of C_2, C_3, and deduce that there would be a group homomorphism $C_2 \times C_3 \to S_3$ with certain properties;
- show that there is no such homomorphism.

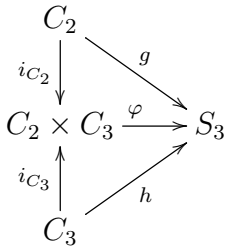
- Monomorphisms $g : C_2 \to S_3$, $h : C_3 \to S_3$ can be constructed as follows:

$$g([0]_2) = e, g([1]_2) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

$$h([0]_3) = e, h([1]_3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, h([2]_3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

- Supposing that $C_2 \times C_3$ is a coproduct of C_2, C_3, there would be a unique group

homomorphism $\varphi : C_2 \times C_3 \to S_3$ such that the following diagram commutes



In other words, for all $a \in C_2, b \in C_3$,

$$\begin{aligned}\varphi(a,b) &= \varphi(([0]_2,b)+(a,[0]_3)) = \varphi(([0]_2,b))\varphi((a,[0]_3)) = \varphi(i_{C_3}(b))\varphi(i_{C_2}(a)) = h(b)g(a)\\ &= \varphi((a,[0]_3)+([0]_2,b)) = \varphi((a,[0]_3))\varphi(([0]_2,b)) = \varphi(i_{C_2}(a))\varphi(i_{C_3}(b)) = g(a)h(b).\end{aligned}$$

- Since
$$g([1]_2)h([1]_3) = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$
$$h([1]_3)g([1]_2) = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
we see $g(a)h(b) \neq h(b)g(a)$ not always holds. The derived contradiction shows that $C_2 \times C_3$ is not a coproduct of C_2, C_3 in Grp.

∎

3.7 Show that there is a surjective homomorphism $Z * Z \to C_2 * C_3$. ($*$ denotes coproduct in Grp.)

Consider the mapping

$$\begin{aligned}\varphi : \mathbb{Z} * \mathbb{Z} &\longrightarrow C_2 * C_3\\ x^{m_1}y^{n_1}\cdots x^{m_k}y^{n_k} &\longmapsto x^{[m_1]_2}y^{[n_1]_3}\cdots x^{[m_k]_2}y^{[n_k]_3}\end{aligned}$$

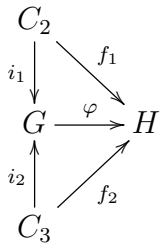
Since

$$\begin{aligned}&\varphi(x^{m_1}y^{n_1}\cdots x^{m_k}y^{n_k}x^{m'_1}y^{n'_1}\cdots x^{m'_{k'}}y^{n'_k})\\ =&x^{[m_1]_2}y^{[n_1]_3}\cdots x^{[m_k]_2}y^{[n_k]_3}x^{[m'_1]_2}y^{[n'_1]_3}\cdots x^{[m'_k]_2}y^{[n'_k]_3},\\ =&\varphi(x^{m_1}y^{n_1}\cdots x^{m_k}y^{n_k})\varphi(x^{m'_1}y^{n'_1}\cdots x^{m'_{k'}}y^{n'_k})\end{aligned}$$

φ is a homomorphism. It is clear that φ is surjective. Thus we show there exists a surjective homomorphism $Z * Z \to C_2 * C_3$. ∎

3.8 Define a group G with two generators x, y, subject (only) to the relations $x^2 = e_G, y^3 = e_G$. Prove that G is a coproduct of C_2 and C_3 in Grp. (The reader will obtain an even more concrete description for $C_2 * C_3$ in Exercise 9.14; it is called the modular group.) [§3.4, 9.14]

Given the maps $i_1 : C_2 \to G, [m]_2 \mapsto x^m$ and $i_2 : C_3 \to G, [n]_3 \mapsto y^n$, we can check that i_1, i_2 are homomorphisms. We are to show that for every group H endowed with two homomorphisms $f_1 : C_2 \to H$, $f_2 : C_3 \to H$, there would be a unique group homomorphism $\varphi : G \to H$ such that the following diagram commutes



or

$$\varphi(i_1([m]_2)) = \varphi(x^m) = \varphi(x)^m = f_1([m]_2),$$
$$\varphi(i_2([n]_3)) = \varphi(y^n) = \varphi(y)^n = f_2([n]_3).$$

Define $\phi : G \to H$ as $\phi(x^m y^n) = f_1([m]_2) f_2([n]_3)$, $\phi(y^n x^m) = f_2([n]_3) f_1([m]_2)$. It is clear to see ϕ makes the diagram commute. Moreover, if φ makes the diagram commute, it follows that for all $x^m y^n, y^n x^m \in G$,

$$\varphi(x^m y^n) = \varphi(x^m)\varphi(y^n) = f_1([m]_2) f_2([n]_3),$$

$$\varphi(y^n x^m) = \varphi(y^n)\varphi(x^m) = f_2([n]_3) f_1([m]_2),$$

which implies $\varphi = \phi$. Thus we can conclude G is the coproduct of C_2 and C_3 in Grp.

■

§4. Group homomorphisms

4.1 Check that the function π_m^n defined in §4.1 is well-defined, and makes the diagram commute. Verify that it is a group homomorphism. Why is the hypothesis $m|n$ necessary? [§4.1]

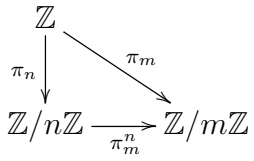
In §4.1 the function π_m^n is defined as

$$\begin{aligned} \pi_m^n \ : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ [a]_n &\longmapsto [a]_m \end{aligned}$$

with the condition $m|n$. We can check that π_m^n is well-defined as

$$[a_1]_n = [a_2]_n \iff a_1 - a_2 = kn = (kl)m \implies [a_1]_m = [a_2]_m \iff \pi_m^n([a_1]_n) = \pi_m^n([a_2]_n).$$

Note $\pi_m^n(\pi_n(a)) = \pi_m^n([a]_n) = [a]_m = \pi_m(a)$. The diagram in §4.1 must commute.



Since

$$\pi_m^n([a]_n + [b]_n) = [a+b]_m = [a]_m + [b]_m = \pi_m^n([a]_n) + \pi_m^n([b]_n),$$

it follows that π_m^n is a group homomorphism. Actually we have shown that without the hypothesis $m|n$, π_m^n may not be well-defined. ∎

4.2 Show that the homomorphism $\pi_2^4 \times \pi_2^4 : C_4 \to C_2 \times C_2$ is not an isomorphism. In fact, is there any nontrivial isomorphism $C_4 \to C_2 \times C_2$?

Let calculate the order of each non-zero element in both C_4 and $C_2 \times C_2$. For the group C_4,

$$|[2]_4| = 2, \quad |[1]_4| = |[3]_4| = 4.$$

For the group $C_2 \times C_2$,

$$|([1]_2, [0]_2)| = |([0]_2, [1]_2)| = |([1]_2, [1]_2)| = 2.$$

Since isomorphism must preserve the order, we can assert that there is no such isomorphism $C_4 \to C_2 \times C_2$. ∎

4.3 Prove that a group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if and only if it contains an element of order n. [§4.3]

Assume some group G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Since $|[1]_n| = n$ and isomorphism preserves the order, we can affirm that there is an element of order n in G.
Conversely, assume there is a group G of order n in which g is an element of order n. By definition we see $g^0, g^1, g^2 \cdots g^{n-1}$ are distinct pairwise. Noticing group G has exactly n elements, G must consist of $g^0, g^1, g^2 \cdots g^{n-1}$. We can easily check that the function

$$\begin{aligned} f \ : G &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ g^k &\longmapsto [k]_n \end{aligned}$$

is an isomorphism. ∎

4.4 Prove that no two of the groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are isomorphic to one another. Can you decide whether $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are isomorphic to one another? (Cf. Exercise VI.1.1.)

Suppose there exists an isomorphism $f : \mathbb{Z} \to \mathbb{Q}$. Let $f(1) = p/q$ $(p, q \in \mathbb{Z})$. If $p = 1$, for all $n \in \mathbb{Z}$, we have

$$f(n) = \frac{n}{q} \neq \frac{1}{2q}.$$

If $p \neq 1$, for all $n \in \mathbb{Z}$, we have

$$f(n) = \frac{np}{q} \neq \frac{p+1}{q}.$$

In both cases, it implies $f(\mathbb{Z}) \nsubseteq \mathbb{Q}$. Hence we see f is not a surjection, which contradicts the fact that $f : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Compare the cardinality of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

$$|\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$$

and we show there exists no such isomorphisms like $f : \mathbb{Z} \to \mathbb{R}$ or $f : \mathbb{Q} \to \mathbb{R}$.
We can prove $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are isomorphic, if considering the both as vector spaces over $\mathbb{Q}$.

■

4.5 Prove that the groups $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are not isomorphic.

Suppose $f : \mathbb{R} \to \mathbb{C}$ is an isomorphism. Then there exists a real number x such that $f(x) = i$.

$$f(x^4) = f(x)^4 = i^4 = 1.$$

Since isomorphism preserves the identity, we have

$$f(1) = 1 = f(x^4).$$

which indicates $x^4 = 1$. Noticing that $x \in \mathbb{R}$, there must be $x^2 = 1$. Now we see

$$f(1) = f(x^2) = f(x)^2 = i^2 = -1,$$

which derives a contradiction. Thus we can conclude that groups $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are not isomorphic.

■

4.6 We have seen that $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ are isomorphic (Example 4.4). Are the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \cdot)$ isomorphic?

Suppose $f : \mathbb{Q} \to \mathbb{Q}_{>0}$ is an isomorphism. Since isomorphism preserves the multiplication, we have

$$f(1) = f\left(n \cdot \frac{1}{n}\right) = f\left(\frac{1}{n}\right)^n \quad (n \in \mathbb{Z}_{>0}),$$

which implies

$$f\left(\frac{1}{n}\right) = f(1)^{\frac{1}{n}}.$$

Assume $f(1) = \dfrac{p}{q} = \dfrac{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}{q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l}}$ where p_i, q_i are pairwise distinct positive prime numbers. Then let $M = \max\{p, q\} + 1 > \max\{r_1, \cdots, r_k, s_1, \cdots, s_l\}$. Thus we assert

$$f\left(\frac{1}{M}\right) = \left(\frac{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}{q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l}}\right)^{\frac{1}{M}} \notin \mathbb{Q},$$

which can be proved by contradiction. Suppose

$$\left(\frac{p}{q}\right)^{\frac{1}{M}} = \frac{a}{b} \in \mathbb{Q}$$

or say

$$pb^M = qa^M,$$

where a, b are coprime. Note b^M, a^M are also coprime and the prime factorization of a^M can be written as $a_1^{Mt_1} a_2^{Mt_2} \cdots a_j^{Mt_j}$ where a_i are pairwise distinct positive prime numbers. That forces

$$p = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = N \cdot a_1^{Mt_1} a_2^{Mt_2} \cdots a_j^{Mt_j}.$$

Noticing that a_i must coincide with one number in $\{p_1, p_2, \cdots p_k\}$, we can assume $a_1 = p_1$ without loss of generality. However, since $M > \max\{r_1, \cdots, r_k\}$, we see the exponent of p_1 is distinct from that of a_1, which violates the unique factorization property of $\mathbb{Z}$. Hence we get a contradiction and conclude $f\left(\frac{1}{M}\right) \notin \mathbb{Q}$. Moreover, it contradicts our assumption that $f : \mathbb{Q} \to \mathbb{Q}_{>0}$ is an isomorphism. Eventually we show that the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \cdot)$ are not isomorphic.

■

4.7 Let G be a group. Prove that the function $G \to G$ defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian. Prove that $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Given the function

$$\begin{aligned} f \ : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

we have

$$f(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}, \quad f(g_1) f(g_2) = g_1^{-1} g_2^{-1}.$$

If G is abelian, it is clear to see $f(g_1 g_2) = f(g_1) f(g_2)$. If f is a homomorphism, $\forall h_1, h_2 \in G$,

$$h_1 h_2 = (h_2^{-1} h_1^{-1})^{-1} = f(h_2^{-1} h_1^{-1}) = f(h_2^{-1}) f(h_1^{-1}) = h_2 h_1.$$

Given the function

$$\begin{aligned} h \ : G &\longrightarrow G \\ g &\longmapsto g^2 \end{aligned}$$

we have

$$h(g_1g_2) = (g_1g_2)^2 = g_1g_2g_1g_2, \quad h(g_1)h(g_2) = g_1^2g_2^2 = g_1g_1g_2g_2.$$

If G is abelian, it is clear to see $h(g_1g_2) = h(g_1)h(g_2)$. If h is a homomorphism, by cancellation we have

$$h(g_1g_2) = h(g_1)h(g_2) \implies g_2g_1 = g_1g_2.$$

■

4.8 Let G be a group, and $g \in G$. Prove that the function $\gamma_g : G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms γ_g are called 'inner' automorphisms of G.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian.

Since

$$\gamma_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b),$$

γ_g is an automorphism of G. For all $a \in G$, we have

$$\gamma_{g_1g_2}(a) = g_1g_2ag_2^{-1}g_1^{-1} = \gamma_{g_1}(g_2ag_2^{-1}) = (\gamma_{g_1} \circ \gamma_{g_2})(a),$$

which implies $\gamma_{g_1g_2} = \gamma_{g_1} \circ \gamma_{g_2}$ and $g \mapsto \gamma_g$ is a homomorphism. If G is abelian, for all g the homomorphism

$$\gamma_g(a) = gag^{-1} = gg^{-1}a = a$$

is the identity in $\mathrm{Aut}(G)$. That is, the homomorphism $g \mapsto \gamma_g$ is trivial. If the homomorphism $g \mapsto \gamma_g$ is trivial, we have for all $g, a \in G$,

$$gag^{-1} = a,$$

which implies for all $a, b \in G$,

$$ab = bab^{-1}b = ba.$$

Thus we show the homomorphism $g \mapsto \gamma_g$ is trivial if and only if G is abelian. ■

4.9 Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$.

Define a function

$$\begin{aligned} \varphi \ &: C_m \times C_n \longrightarrow C_{mn} \\ &([a]_m, [b]_n) \longmapsto [anp + bmq]_{mn} \end{aligned}$$

where $[pn]_m = [1]_m$ and $[qm]_n = [1]_n$, as $\gcd(m, n) = 1$ guarantees the existence of p, q (see textbook p56). First of all, we have to check whether φ is well-defined. Note that

$$[(anp_1 + bmq_1) - (anp_2 + bmp_2)]_m = [a(p_1n - p_2n) + b(q_1m - q_2m)]_m = [0]_m$$

$$[(anp_1 + bmq_1) - (anp_2 + bmp_2)]_n = [a(p_1n - p_2n) + b(q_1m - q_2m)]_n = [0]_n$$

and $\gcd(m,n)=1$. Thus we have

$$[(anp_1+bmq_1)-(anp_2+bmp_2)]_{mn}=[0]_{mn},$$

or

$$[anp_1+bmq_1]_{mn}=[anp_2+bmp_2]_{mn}.$$

Then we show φ is a homomorphism.

$$\begin{aligned}\varphi(([a_1]_m,[b_1]_n)+([a_2]_m,[b_2]_n)) &= \varphi([a_1+a_2]_m,[b_1+b_2]_n)\\ &= [(a_1+a_2)np+(b_1+b_2)mq]_{mn}\\ &= [a_1np+b_1mq]_{mn}+[a_2np+b_2mq]_{mn}\\ &= \varphi([a_1]_m,[b_1]_n)+\varphi([a_2]_m,[b_2]_n).\end{aligned}$$

In order to show φ is a monomorphism, we can check

$$\begin{aligned}&\varphi([a_1]_m,[b_1]_n)=\varphi([a_2]_m,[b_2]_n)\\ \Longrightarrow\ &[a_1np+b_1mq]_{mn}=[a_2np+b_2mq]_{mn}\\ \Longrightarrow\ &[(a_1-a_2)np+(b_1-b_2)mq]_{mn}=[0]_{mn}\\ \Longrightarrow\ &[(a_1-a_2)np+(b_1-b_2)mq]_m=[a_1-a_2]_m=[0]_m,\\ &[(a_1-a_2)np+(b_1-b_2)mq]_n=[b_1-b_2]_n=[0]_n\\ \Longrightarrow\ &[a_1]_m=[a_2]_m,\ [b_1]_m=[b_2]_m.\end{aligned}$$

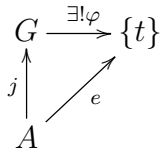
Since $|C_m\times C_n|=|C_{mn}|=mn$, we can conclude φ is an isomorphism. Thus we complete proving $C_{mn}\cong C_m\times C_n$.

∎

§5. Free groups

5.1 Does the category $\mathscr{F}^A$ defined in §5.2 have final objects? If so, what are they?

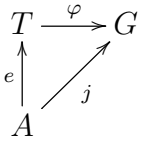
Yes, they are functions from A to any trivial group, for example $T=\{t\}$.



For any object (j,G) in $\mathscr{F}^A$, the trivial homomorphism $\varphi: g\mapsto t$ is the unique homomorphism such that the diagram commutes. That is, $\mathrm{Hom}((j,G),(e,T))=\{\varphi\}$. ∎

5.2 Since trivial groups T are initial in Grp, one may be led to think that (e, T) should be initial in $\mathscr{F}^A$, for every A: e would be defined by sending every element of A to the (only) element in T ; and for any other group G, there is a unique homomorphism $T \to G$. Explain why (e, T) is not initial in $\mathscr{F}^A$ (unless $A = \emptyset$).

Let $G = C_2 = \{[0]_2, [1]_2\}$. Note that $\varphi \circ e(A)$ must be the trivial subgroup $\{[0]_2\}$. If $x \in A$ and $j(x) = [1]_2$, we see $\varphi \circ e \neq j$ and the following diagram does not commute.



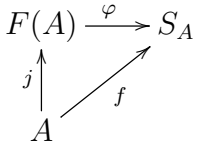
That implies (e, T) is not initial in $\mathscr{F}^A$ unless $A = \emptyset$. ∎

5.3 Use the universal property of free groups to prove that the map $j : A \to F(A)$ is injective, for all sets A. (Hint: it suffices to show that for every two elements a, b of A there is a group G and a set-function $f : A \to G$ such that $f(a) = f(b)$. Why? and how do you construct f and G?) [§III.6.3]

Let $G = S_A$ be the symmetric group over A. Define functions $g_a : A \to A,\ x \mapsto a$ sending every element of A to a. Since $g_a \in S_A$, we can define an injection

$$\begin{aligned} f\ : A &\longrightarrow S_A \\ a &\longmapsto g_a \end{aligned}$$

In light of the commuting diagram



we have $\forall a, b \in A$,

$$j(a) = j(b) \implies \varphi(j(a)) = \varphi(j(b)) \implies f(a) = f(b) \implies a = b.$$

∎

5.4 In the 'concrete construction of free groups, one can try to reduce words by performing cancellations in any order; the 'elementary reductions' used in the text(that is, from left to right) is only one possibility. Prove that the result of iterating cancellations on a word is independent of the order in which the cancellations are performed. Deduce the associativity of the product in $F(A)$ from this. [§5.3]

We use induction on the length of w. If w is reduced, there is nothing to show. If not, there must be some pair of symbols that can be cancelled, say the underlined pair

$$w = \cdots \underline{xx}^{-1} \cdots .$$

(Let's allow x to denote any element of A', with the understanding that if $x = a^{-1}$ then $x^{-1} = a$.) If we show that we can obtain every reduced form of w by cancelling the pair xx^{-1} first, the proposition will follow by induction, because the word $w^* = \cdots \cancel{\underline{xx}^{-1}} \cdots$ is shorter.

Let w_0 be a reduced form of w. It is obtained from w by some sequence of cancellations. The first case is that our pair xx^{-1} is cancelled at some step in this sequence. If so, we may as well cancel xx^{-1} first. So this case is settled. On the other hand, since w_0 is reduced, the pair xx^{-1} can not remain in w_0. At least one of the two symbols must be cancelled at some time. If the pair itself is not cancelled, the first cancellation involving the pair must look like

$$\cdots \cancel{x}^{-1} \underline{\cancel{x}x}^{-1} \cdots \qquad \text{or} \qquad \cdots \underline{x\cancel{x}}^{-1} \cancel{x} \cdots$$

Notice that the word obtained by this cancellation is the same as the one obtained by cancelling the pair xx^{-1}. So at this stage we may cancel the original pair instead. Then we are back in the first case, so the proposition is proved.

■

5.5 Verify explicitly that $H^{\oplus A}$ is a group.

Assume the A is a set and H is an abelian group. $H^{\oplus A}$ are defined as follows

$$H^{\oplus A} := \{\alpha : A \to H | \alpha(a) \neq e_H \text{ for only finitely many elements } a \in A\}.$$

Now that $H^{\oplus A} \subset H^A := \mathrm{Hom}_{\mathsf{Set}}(A, H)$, we can first show $(H^A, +)$ is a group, where for all $\phi, \psi \in H^A$, $\phi + \psi$ is defined by

$$(\forall a \in A) : (\phi + \psi)(a) := \phi(a) + \psi(a).$$

Here is the verification:

- Identity: Define a function $\varepsilon : A \to H, a \mapsto e_H$ sending all elements in A to e_H. Then for any $\alpha \in H^A$ we have

  $$(\forall a \in A) : (\alpha + \varepsilon)(a) = \alpha(a) + \varepsilon(a) = \alpha(a),$$

  which is $\alpha + \varepsilon = \alpha$. Because of the commutativity of the operation $+$ defined on H^A, ε is the identity indeed.

- Associativity: This follows by the associativity in H:

  $$(\forall a \in A) : ((\alpha+\beta)+\gamma)(a) = (\alpha+\beta)(a)+\gamma(a) = \alpha(a)+(\beta+\gamma)(a) = (\alpha+(\beta+\gamma))(a).$$

- Inverse: Every function $\phi \in H^A$ has inverse $-\phi$ defined by

$$(\forall a \in A) : (-\phi)(a) = -\phi(a).$$

Thus H^A makes a group.

Then it is time to show $H^{\oplus A}$ is a subgroup of H^A. For all $\alpha, \beta \in H^{\oplus A}$, let $N_\alpha = \{a \in A | \alpha(a) \neq e_H\}$, $N_\beta = \{a \in A | \beta(a) \neq e_H\}$, $N_{\alpha-\beta} = \{a \in A | (\alpha - \beta)(a) \neq e_H\}$. Since

$$(\forall a \in A) : (\alpha - \beta)(a) = \alpha(a) - \beta(a),$$

we have

$$(\alpha - \beta)(a) \neq e_H \implies \alpha(a) \neq e_H \text{ or } \beta(a) \neq e_H,$$

which implies $N_{\alpha-\beta} \subset N_\alpha \cup N_\beta$. Note that N_α, N_β are both finite sets, which forces $N_{\alpha-\beta}$ to be finite. So there must be $\alpha - \beta \in H^{\oplus A}$. Now we see $H^{\oplus A}$ is closed under additions and inverses. And $e_{H^A} = \varepsilon \in H^{\oplus A}$ means that $H^{\oplus A}$ is nonempty. Finally we can conclude $H^{\oplus A}$ is a subgroup of H^A. ∎

References