Algebra

I. Set Theory and Categories

1. Sets and Categories

1.1

Suppose that for any property, we can define a set whose members are items that satisfy that property. Then let $r = \{x : x \notin x\}$. Then $r \in r \iff r \notin r$.

In naive set theory and ZFC, this is avoided as the axiom schema of specification (for any property P and set S the set S is satisfies S exists) requires an existing set S. Also, a set of all sets cannot exist, as otherwise we can take S to be such a set.

1.2

Nonempty: any equivalence class [a] contains a.

Disjoint: we wish to show that $[a] \neq [b] \implies [a] \cap [b] = \{\}$. Equivalently, $[a] \cap [b] \neq \{\} \implies [a] = [b]$. Suppose $c \in [a] \cap [b]$, and let $a' \in [a]$. Then $a' \sim a \sim c \sim b$, hence $[a] \subseteq [b]$. Similarly $[b] \subseteq [a]$.

Union is S: S contains the union as it contains every equivalence class by construction. Let $s \in S$. Then $s \in [s]$, hence the union contains S.

1.3

Define $a \sim b$ when there exists $p \in P$ such that $a \in p, b \in p$.

1.4

We count partitions. A partition will have 1, 2 or 3 parts. If it has 1 part it must be the whole set and if it has 3 parts it must be $\{[1], [2], [3]\}$. If it has 2 parts, exactly one part will have 2 items and the other 1 item, and we have 3 choices for the singleton part. Hence there are 5 equivalence relations.

1.5

For $a, b \in \mathbb{R}$ define $a \sim b$ when |a - b| < 2. Then $0 \sim 1$ and $1 \sim 2$ but $0 \not\sim 2$.

1.6

Reflexive: for $r \in \mathbb{R}$ we have $r \sim r$ since $r - r = 0 \in \mathbb{Z}$.

Symmetric: suppose $a \sim b$. Then $a - b \in \mathbb{Z}$. Then $b - a = -(b - a) \in \mathbb{Z}$, hence $b \sim a$.

Transitive: suppose $a \sim b, b \sim c$. Then $a - c = (a - b) + (b - c) \in \mathbb{Z}$.

Every class in \mathbb{R}/\sim is represented by a unique real number $r\in[0,1)$, which is equivalent to all real numbers with that fractional part.

Every class in \mathbb{R}^2/\approx is represented by a unique pair of real numbers (r_1, r_2) with each $r_i \in [0, 1)$, which is equivalent to all pairs of real numbers whose fractional parts are the representative.

1. Functions between sets

2.1

n!

2.2

Let $f: A \to B$. We wish to show that f has a right-inverse iff it is surjective.

 \implies : let $b \in B$. Suppose the right inverse is g; then $f \circ g = id_B$ hence $b = f(g(b)) \in f(A)$.

 \Leftarrow : we define $g: B \to A$ as follows. Let $b \in B$. Choose $a \in f^{-1}(b)$, which is nonempty since f is surjective, then set g(b) = a. Then g is a right inverse. Proof: for all $b \in B$ we have f(g(b)) = f(a) = b.

2.3

Let $f: A \to B$ be a bijection and f^{-1} its inverse. Since f^{-1} is a right inverse of f, we have $f \circ f^{-1} = id_B$ hence f is a left inverse of f^{-1} . Similarly it is a right inverse as well; hence f^{-1} is a bijection.

Let $g: A \to B, f: B \to C$ be bijections. Then $(f \circ g) \circ (g^{-1} \circ f^{-1}) = id_C$, hence $f \circ g$ is surjective. Similarly, it is injective.

2.4

Reflexive: for any set A, |A| = |A| since id_A is a bijection.

Symmetric: suppose |A| = |B|, that is, there is a bijection $f: A \to B$. Then $f^{-1}: B \to A$ is a bijection, hence |B| = |A|.

Transitive: suppose |A| = |B|, |B| = |C| with bijections f and g. Then $f \circ g$ is a bijection between A and C.

2.5

A function $f:A\to B$ is an epimorphism (is epic) if for all sets Z and all functions $\alpha',\alpha'':B\to Z$ we have $\alpha'\circ f=\alpha''\circ f\implies \alpha'=\alpha$. A function is surjective iff it is epic.

 \implies : Let $f: A \to B$ be surjective and $\alpha', \alpha'': B \to Z$ such that $\alpha' \circ f = \alpha'' \circ f$. Then f has a right inverse g and $\alpha' \circ f \circ g = \alpha'' \circ f \circ g$. Hence $\alpha' = \alpha''$.

 \Leftarrow : Let $f: A \to B$ be epic and let $b \in B$. We wish to show that $b \in f(A)$. Let $Z = \{0, 1\}$ and suppose α' and α'' disagree only on b, that is, $\alpha'(c) = \alpha''(c) \iff c \neq b$. Then $\alpha' \neq \alpha''$. Suppose $b \notin f(A)$. Then for all $a \in A\alpha' \circ f(a) = \alpha'' \circ f(a)$ (proof: $f(a) \neq b$, hence $\alpha'(f(a)) = \alpha''(f(a))$), which contradicts f is an epimorphism.

2.6

For any $f: A \to B$ define $\phi_f: A \to A \times B$ by $\phi_f(a) = (a, f(a))$. Then ϕ_f is a section (right inverse) of π_A . Proof: for all $a \in A$ we have $\pi_A \circ \phi_f(a) = \pi_A(a, f(a)) = a$. In fact every section of π_A corresponds to a unique function, since the $\pi_B(\pi_A^{-1}(x)) = B$.

2.7

For all $f: A \to B$ let $\phi_f: A \to \Gamma_f$ be given by $\phi(a) = (a, f(a))$. Then π_A is a left inverse of ϕ_f by exercise 2.6, hence ϕ_f is injective. Also ϕ_f is surjective. Proof: suppose $y = (a, b) \in \Gamma_f$. Then b = f(a), hence $y = \phi_f(a)$.

2.8

The equivalence relation is: $r_1 \sim r_2 \iff e^{2\pi i r_1} = e^{2\pi i r_2} \iff r_1 - r_2 \in \mathbb{Z}$. Hence the surjection maps r to (the equivalence class represented by) its fractional part; \bar{f} maps [r] to $e^{2\pi i r}$, with the unit circle as codomain; the injection is the inclusion map (of the unit circle in the complex plane).

2.9

Let the bijection between A' and A'' be f and the bijection between B' and B'' be g. Define a bijection $h: A' \cup B' \to A'' \cup B''$ as follows: h(x) is f(x) if $x \in A'$ otherwise g(x). This is well-defined as exactly one of $x \in A', x \in B'$ is true. The inverse can be defined explicitly similarly.

To form the disjoint union of A and B be produce disjoint copies; suppose we do this in one way to get A' and B', and another way to get A'' and B''. Since they are copies, $A' \cong A'', B' \cong B''$, hence the disjoint unions are isomorphic (as sets).

2.10

Any function from A to B is defined by the value of f(a) for all $a \in A$; the choice for each a is independent, there are |A| choices and for each choice we may choose |B| ways, so there are $|A| \times |A| \times \ldots |A|$ different functions.

For an explicit bijection, we can use the fact that any finite set can be well-ordered to order the elements of $|B^A|$ lexicographically on their valuations $(f(a_1), f(a_2)...)$.

2.11

A subset $S \subseteq A$ is determined uniquely by its indicator function $f_S \in 2^A$ given by $f_S(a) = 0 \iff a \in S$.

3. Categories

3.1

We compose two morphisms in C^{op} by composing the two underlying morphisms in C "the other way". That is, suppose $f \in \operatorname{Hom}_{C^{op}}(A,B) = \operatorname{Hom}_C(B,A)$ and $g \in \operatorname{Hom}_{C^{op}}(B,C) = \operatorname{Hom}_C(C,B)$. Let composition in C be denoted by \cdot and composition in C^{op} by \circ . Then define their composition $g \circ f = f \cdot g$.

- 1. The identity homorphism exists because $1_A \in \operatorname{Hom}_C(A,A) = \operatorname{Hom}_{C^{op}}(A,A)$.
- 2. We explicitly constructed the composition in C^{op} , hence it exists.
- 3. $(f \circ g) \circ h = h \cdot (g \cdot f) = (h \cdot g) \cdot f = f \circ (g \circ h)$.
- 4. $f \circ 1_A = 1_A \cdot f = f$; similar proof for left inverse.

3.2

$$|\operatorname{End}(A)| = |\operatorname{Hom}(A, A)| = |A^A| = |A|^{|A|}.$$

3.3

That means it is a left and right identity. Left identity means for all morphisms $f: a \to b, 1_b f = f$. Proof that 1_b is a left identity: let $f: a \to b$. By our definition of composition, $1_b f = (a, b)$ (let c = b on p21), which is identically f. The proof for right identity is similar.

3.4

No, since $n \not< n$, so Hom(n, n) is empty.

3.5

 \subseteq in 3.4 is the \sim relation in 3.3 (that is required to be reflexive and transitive).

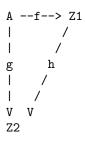
3.6

- 1. Let the identity in V be the identity matrix.
- 2. Let $f: x \to y, g: y \to z$. The composition gy is exactly the matrix product gy, which is the correct size $(gy: x \to z \text{ is a } z \times y \text{ matrix})$.
- 3. Associativity follows from associativity of matrix multiplication.
- 4. The identity matrix is an identity with respect to matrix multiplication.

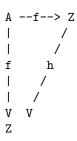
An object n of this category can be thought of as \mathbb{R}^n , and the morphisms $\mathrm{Hom}(m,n)$ as linear functions $\mathbb{R}^m \to \mathbb{R}^n$. (Eg use the standard basis on \mathbb{R}^m and \mathbb{R}^n to convert a linear function to an appropriately sized matrix).

Let us denote this category as C^A . Then the objects of C^A are morphisms of C. Given two objects in $f,g \in Obj(C^A)$, suppose $f \in \operatorname{Hom}_C(A,Z_1)$ and $g \in \operatorname{Hom}_C(A,Z_2)$. Define a C^A -morphism from f to g to be a C-morphism h such that the diagram commutes.



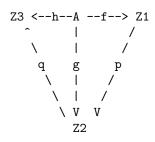


1. An identity C^A -morphism on the C^A -object f is a C-morphism h such that

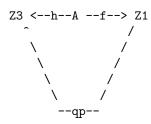


commutes; 1_Z does the job.

2. Suppose f, g, h are C^A -objects and p is a C^A -morphism from f to g and q is a C^A -morphism from g to h. Then the following diagram commutes.



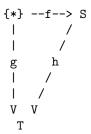
By removing the vertical line and composing p and q,



commutes; hence define composition in C^A as composition in C.

3. Associativity follows from associativity in C.

We will also verify the claim in example 3.8.



The requirement is that h commutes, that is, considered as set-functions, $g = h \circ f$. Since g is completely determined by its value on *, this means g(*) = h(f(*)), or t = h(s).

3.8

The objects of C are infinite sets and the morphisms in C are set-functions between them (that is we define $\operatorname{Hom}_{C}(A,B) = \operatorname{Hom}_{Set}(A,B)$, forcing C to be a full subcategory of Set). Identity, composition and associativity all follow from Set.

3.9

WIP

A function maps between two sets; we must generalize this concept to allow for maps between two multisets. How we do this determines the structure of morphisms in MSet. (In all cases, though, members of Obj(MSet) will be pairs (S, \sim) where \sim is an equivalence relation on S).

- 1. We can treat (S, \sim) as a partitioned set; then mfunctions between them will be functions between partitions.
- 2. We can simply inherit the morphisms from S, allowing morphisms to ignore \sim altogether. The downside is that mfunctions are now sensitive to which representative of a given element you feed it.
- 3. We can generalize functions to "multivalued functions" (eg the $z \to z^{1/3}$ operator on \mathbb{C}); TBD
- 4. We can generalize functions to "regular functions whose image contain elements with multiplicities"; for finite multiplicities this is like a regular function $x \to (y, n)$ where x, y are our conceptual domain and codomain and n is the multiplicity. A contrived example is: given a fixed function f over \mathbb{R} , we could map x to (y, n) where y = f(x) and n is the algebraic multiplicity of the root of the function f'(t) = f(t) f(x) at y (hence n would mostly be 1, and at stationary points it would increase).

3.10

The object $\Omega = \{0,1\}$ will do. A subobject (subset) A' of an object (set) A can be identified with a morphism (set-function) $f: A \to \Omega$ by setting $a \in A' \iff f(a) = 1$.

3.11

TBD

4. Morphisms
4.1
No.
4.2
4.3
4.4
TBD
The nonmono version cannot work since the identity is a monomphism (hence not a nonmomorphism)
4.5
TBD