General sets and operations

vishvAs vAsuki

November 24, 2011

Contents

Part I

Prelude

1 Notation

'Algebra about strucure and equalities. Analysis about inequalities.'
Entire/ Integral function is holo morphic (differentiable) on entire complex plane.

2 Research Themes

Properties of various algebraic objects, their relationships.

2.1 Characterization of research effort

See linear algebra survey, complexity theory survey.

3 Algebra techniques

3.1 Symbol manipulation, abstraction

Algebra is about correct reasoning: symbol manipulation according to some rules.

3.1.1 Abstraction: sub expressions

It is about abstraction by means of techniques such as **change of variables**.
Look for structure in expressions, understand and if necessary, abstract away sub-expressions with new variables: very important! ***Too many symbols can slow down cognition!***
Use properties of algebraic objects well, keep a list of such properties handy.

3.2 Common proof techniques

Induction. Direct inference.

3.2.1 Contradiction

Diagonalization: Order all elements, make a new element which differs from every other element.

Part II

Sets

4 Set S

4.1 Specification

Use vectors $\in \{0,1\}^n$. Or use an indicator function: $I_S(x) = 1$ if $x \in S$.

4.1.1 Variants

Multiset/ Bag: set with repeats. Class: set of sets.

4.2 Operations

$\cup, \cap, -, \Delta$; universal set U.

4.2.1 Product

Set (Cartesian) product of sets, $A \times B = \{(a,b) | a \in A \wedge b \in B\}$.
Subsets of product of sets, or relations, are considered elsewhere.

4.2.2 Disjoint union

A union of disjoint sets, with each element subscripted by the set it originates from.

4.2.3 Properties

Connections to logic: De Morgan laws.

4.3 Impossible sets

S : set of all sets which are not members of themselves: See if S is a member of itself.

4.4 Metric spaces and topology

See topology survey.

4.5 Partition of set S

A mutually disjoint $\{S_i\}$ such that $\cup_i S_i = S$.

5 Orders over set S

5.1 Total order

All $(x, y) \in S$ comparable.

5.1.1 Minimum element

$\forall y \in S : x \leq y$.

5.2 Partial order

Aka Posets: Partially Ordered sets. Maybe some $(x, y) \in S$ not comparable. Eg: vectors, componentwise $<$. Visualize with Hasse diagrams.

5.2.1 Minimal element

$\forall y \in S : x \leq y \implies x = y$. Note difference from minimum. Eg: in triangle joining (1,1), (0, 1), (1, 0): line joining the last 2 pts are minimal elements.

5.3 Bounds on A, subset of S

Upper and lower bounds: need not be in A.
Supremum or least upper bound or GLB or join. Infimum or greatest lower bound or LUB or meet.

5.3.1 Difference from max and min

$\max(A) \in A \subseteq S$ always, but $\sup(A) \notin A, \sup(A) \in S$ possible.

5.3.2 Supremum property in S

S with supremum property: For any $A \subseteq S : \exists \sup A \in S$.
If S has supremum property, it has infemum property: For any subset $A \neq S$, take S-A and find its supremum.

5.3.3 Examples

Q does not have supremum property, but R does. See complex analysis survey.

5.4 Lattices

Sets where every pair has a same supremum and same infemum: Diamond.

5.5 Well founded order

Take any 'decreasing chain' $a < b < c..$: it must be finite. So, $a < a$ not allowed, no cycles too. Not total or partial order: no transitivity etc required. Thence get 'well founded set'. Minimal elements exist.
Eg: $(N, <)$, (strings, psurveyix), (strings, subsequence), (trees, subtree). Lexicographic ordering of $((a, b), <)$ is well founded if $<$ well founded over dom(a) and dom(b).

5.5.1 Mathematical induction proofs generalized

(Noether). If $\forall y :: x > y \land p(y) \implies p(x)$, then $\forall x : p(x)$; note: base cases subsumed here. Strictly more powerful than induction on natural numbers: consider lexicographic ordering.

6 Algebras over sets

6.1 Boolean algebra over set X

Bounded lattice where every element has complement, which is distributive. Eg: power sets wrt inclusion, propositional logic.

6.2 Sigma algebra S over set X

Aka Borel algebra. Let 2^X be the set of powersets of X. Let $S \subseteq 2^X$ be closed under countable unions and complementation.
Note that S is also ***closed under intersection*** due to these conditions: due to De Morgan's laws.
Sigma algebra is a Boolean algebra defined over S with the inclusion operation, extended to unbounded sets.

6.2.1 Importance

The sigma algebra is useful in defining a measurable space.

7 Size

7.1 Measurable space

Suppose that S is a σ algebra over X. (X, S) is called a measurable space. Every member of S is a measurable set.

$(S, 2^S)$ is a common measurable space.

7.1.1 Importance

This notion is useful because it enumerates the sets whose size we want to measure.

7.1.2 Product space

You can take two measurable spaces $(S_1, F_1), (S_2, F_2)$, and, by set product get a bigger measurable space $(S_1 \times S2, F_1 \times F_2)$.

7.2 Measure

7.2.1 Minimal definition

$m : S \to [0, \infty]$, with $m(\phi) = 0$ and the countable additivity property ($A \cap B = \phi \implies m(A \cup B) = m(A) + m(B)$) is called a measure on X of subsets S.
(X, S, m) is called a measure space.

7.2.1.1 Motivation

This measure of size generalizes concepts such as volume/ area/ box measure, mass, time. Especially important measures are the box measure and the probability measure.

7.2.2 Special classes

7.2.2.1 General additivity

For some measures m, any bunch of mutually disjoint sets S_i: $m(\cup_i S_i) = \sum_i S_i$. This is stronger than countable additivity.

7.2.2.2 Finite measures

If X is a countable union of finite measure sets, m is $\sigma-$finite. This is a very common property.

7.2.2.3 Signed measure

If $m(x) < 0$ is allowed, then m is a signed measure.

7.2.3 Null set, almost-everywhereness

If $m(T) = 0$, then T is called a $m-$null set.
A property (eg: $f(x) > 0$) holds 'almost everywhere' if the set of elements for which the property does not hold is a null set. Eg: 'Almost always' in applications of probability.

7.2.4 Size of the union and intersection

7.2.4.1 Inclusion/ exclusion principle

The following holds for any measure which is finite on the sets involved. $|\cup_{i\in V} S_i| = \sum_i |S_i| - \sum_{i\neq j} |S_i \cap S_j| + .. = \sum_{T\subseteq V} (-1)^{|T|+1} |\cap_{i\in T} S_i|$.

7.2.4.2 Bounds

Thence, we have the union upper bound: $m(A\cup B) \leq m(A) + m(B)$. In the case of probabilistic analysis, this is very useful. Aka Boole's inequality.
Intersection lower bound: $m(A\cap B) \geq m(A) + m(B) - 1$. Aka Bonferroni's inequality. [**Proof**]: $m(A\cup B) \leq 1$ with the inclusion-exclusion principle. $\square$
By mathematical induction, $m(\cap_{i\in(1,n)} A_i) \geq \sum_i m(A_i) - (n-1)$.

7.2.4.3 Generalization

(Mobius inversion lemma). Got functions on sets f, g. $[\forall A \subseteq V : f(A) = \sum_{B\subseteq A} g(B)] \equiv [g(B) = \sum_{B\subseteq A} (-1)^{A-B} f(B)]$. [**Check**]Easy algebraic proof.

7.3 Counting measure

The counting measure of A, $|A|$, equals the number of elements in a set.

7.3.1 Counting, combinatorics

See probability survey.

7.4 Cardinality

The concept of Cardinal numbers extends the notion of the counting measure to compare the sizes of even infinite sets. For finite sets, the cardinality equals the counting measure.

7.4.1 Comparison by bijection

Comparison of cardinalities of A and B can be made by making bijections, even if they're ∞ sets: 'Equinumerousness'.

7.4.2 Hierarchy of cardinal numbers

Consider the power set $P(S)$. $|P(S)| > |S|$.

7.5 Cardinalities of compared to N

Cardinality (or power) of the continuum $c = |R|$; $\aleph_0 = |N|$. Continuum hypothesis: $\exists c'? : \aleph_0 < c' < c$.

7.5.1 Countability

S is countable if it can be mapped to N.
Countable unions of countable S still countable: write any S as a row vector, see their sequence as a matrix, draw a zig-zag line to cover all matrix elements. Similarly, see countability of Q.
If S is countable, S^n is countable: use induction: if S^{k-1} countable, for every $a \in S$, $\left\{ba : b \in S^{k-1}\right\}$ is countable; So, their union is also countable.

7.5.2 Show uncountability

Use Cantor's diagonalization.

7.5.3 Infinite (sub)sets' cardinality

(Dedekind): S is ∞ iff $\exists A \{S\}$ with same cardinality as S. [**Proof**]: Finite S can't have such a proper subset. If $|S| = \infty$, get countably ∞ S'; map to N with function f; but map $n \in N$ to $n+1$ with function g, do f^{-1}. $\square$

7.6 Product measure

Consider the product of two measure spaces: $\{(S_i, F_i, m_i) | i \in \{1, 2\}\}$. The product measure: $m(E_1, E_2) = m_1(E_1) \times m_2(E_2) : \forall E_i \in S_i$.
By induction, one can define product measure for the product of arbitrary number of measure spaces.

7.6.1 Importance

This measure finds application in defining, for example, measures for R^n based on the common box measure for R; and in considering measures over the product of ranges of multiple random variables.

7.6.2 Extension to bigger sigma algebra

Consider the product space with an expanded sigma algebra T such that $(F_1 \times F_2) \subseteq T \subseteq 2^{S_1} \times 2^{S_2}$.
For $A \in T$, one can use the product measure m to define the minimum cover measure $m'(A) = \inf\{\sum_i m(B_i) : A \subseteq \cup_i B_i\}$. One can show that this obeys required properties like countable additivity.
This is aka Lebesgue measure.

7.6.2.1 Importance

It forms a natural basis for defining and studying the box integral over product of multiple measure spaces.

7.7 Connecting measures

7.7.1 Absolute continuity

Consider two $\sigma-$finite measures m, n. m is absolutely continuous with n - or m is dominated by n - or $m << n$ if $\forall t \in S : n(t) = 0 \implies m(t) = 0$.
This is equivalent to a definition reminiscent of absolute continuity of functions n, m: $\forall \epsilon, \exists \delta : \forall t : n(t) \leq \delta \implies m(t) \leq \epsilon$. Prior definition implies this because if there $\exists \epsilon, t : m(t) \geq \epsilon \wedge (n(t) \leq \delta \forall \delta)$ then for that t, $m(t) \geq \epsilon$ while $n(t) = 0$.
This notion is important in defining the inter-measure derivative.

7.7.2 Inter-measure Derivative

Aka Radon-Nikodym derivative. For measures $m << n$ over (X, S), a theorem by Radon/ Nikodym says that $\exists f : X \to [0, \infty] : m(t) = \int_{x \in t} f(x)dn$, and that this f is unique almost everywhere wrt n. [**Find proof**]
Note that $m << n$ is necessary: otherwise, for the event E where $n(E) = 0, m(E) \neq 0$, there is no f such that: $m(E) = \int_E f(x)dn$.
This concept is important in defining probability density functions of random variables.

Part III

Relations

8 Relations and functions

8.1 Relations among n sets

8.1.1 Definition

It is a subset of $A_1 \times ..A_n$.
It is a binary relation between $A_1 \times ..A_{n-1}$ and A_n.

8.1.2 Binary relation R on (A, B)

Aka dyadic relation.

8.1.2.1 Definitions/ views

A relation is fully defined by a subset $G \subseteq A \times B$, called the graph of R. So, it is a $R = (A, B, G)$.
It corresponds to a function $2^A \to 2^B$, and to the characteristic function $A \times B \to \{0, 1\}$.
It is a general many-to-many relationship : a directed graph involving the sets.

8.1.2.2 (Co)Domain

A is the domain/ set of departure. B is the co-domain/ set of destination.
Domain of definition is $\{a : a \in A, \exists b \in B : aRb\}$.
range(R) is the subset of B related by R to some element in A.

8.1.2.3 Totality

If ran(f) = codomain(f), f is onto / surjective/ right-total.
If domain of definition = domain, f is left-total.
A correspondence: a binary relation that is both left-total and surjective.

8.1.3 Endo-relations

A relation where the domain = co-domain.
The set of endo-relations is same as the set of directed graphs.

8.1.3.1 Equivalence

Equivalence relations: Reflexive (aRa), symmetric ($aRb \implies bRa$), transitive ($aRb \wedge bRc \implies aRc$).
The set of symmetric relations is the set of undirected graphs.
Equivalence class determined by a set of elements S and equivalence relation R is the set of all elements related to elements in S by R.

8.1.3.2 Congruence

Complement: $A \times B - R$.
Restricting domain/ codomain of the relation, we get other (left/ right) restricted relations.

8.1.3.3 Reduction and closure

Equivalence relation which preserves certain algebraic operators. Eg: Modulo arithmetic preserves +, *, -.

8.1.4 Functions on relation R: A to B

Ensuring or removing all cases of reflexivity, symmetry and transitivity, we get closures and reductions of relations.

8.1.4.1 Inverse

$R^{-1}(b) = \{a : a \in A, R(a) = b\}$.

8.2 Functions/ transformation f

8.2.1 Partial function A to B

Aka functional, right unique.

8.2.1.1 Definition

It is a special binary relation, where every element in A is mapped to at most one element in B.

8.2.1.2 (Co)domain sets

The domain of definition is also called the preimage. The range is also called the image.

8.2.2 (Total) function

A function is a partial function which is left-total.
A function acts. Like an electrical circuit with an input and an output.

8.2.3 Types

If every element in B has at most one preimage, f is said to be One to one / injection.
A bijective function is both injective and surjective.
Also see survey on Analysis of functions over fields.

8.2.4 Vector nature

A finite domain function can be seen as a vector. So can an ∞ domain function. See functional analysis survey.

8.2.5 Domain: Interesting locations

8.2.5.1 Level Set

$\{x|f(x) = c\}$. A 2d contour line for 3d function. See linear algebra survey for geometric properties.
Kernel is the 0 level set.

8.2.5.2 Fixed point

f(w) = w.

8.2.6 Traits of functions from X to X

Idempotence: $f^n(x) = f(x)$. Nilpotence: $\exists n : f^n(x) = 0$.

8.2.7 Measurable function

Consider a function $f : X_1 \to X_2$, where $(X_i, S_i) \forall i \in \{1, 2\}$ are measurable spaces.
f is a measurable function if the preimage $f^{-1}(s \in S_2)$ is a measurable set: a member of S_1. (This is analogous to definition of continuous functions over metric spaces.) So, it preserves some structure - but not fully: not every member of S_1 is represented in S_2 - only a subset is.
This notion is important in defining box integrals and random variables.

8.2.8 Function/ model family

Suppose that $f : X \times W \to Y$. Suppose that $w \in W$ are designated parameters, and $x \in X$ is designated the independent variable. Then,
$\{f_w : X \to Y = f(x, w) | w \in W\}$ is a parametrized family of functions.
Such function families occur frequently, for example, in machine learning.

8.3 Sequence of maps to metric space

Consider $E \subseteq S$.

8.3.1 Pointwise convergence on E

$f_n \to f$ pointwise if $\forall x \in E, \epsilon, \exists N : n > N \implies d(f_n(x), f(x)) < \epsilon$. Visualize geometrically as a sequence of curves which get closer and closer at different rates at different points.

8.3.2 Uniform convergence on E

$f_n \to f$ if $\forall \epsilon, \exists N : n > N \implies$
$\forall x \in E \; d(f_n(x), f(x)) < \epsilon$. $f_n \to f$ uniformly $\equiv \sup_{x \in E} d(f_n(x), f(x)) \to 0$.
Visualize geometrically as a sequence of curves which get closer and closer at all points.
Cauchy criterion: $\forall n, m > N, x : d(f_n(x), f_m(x)) < \epsilon$.

8.3.3 Interesting functions

Point function: f(x) = 1 only if x = a, f(x) = 0 elsewhere.

8.3.3.1 Important functions over R and C

Includes polynomials over fields. See complex analysis survey.

8.3.3.2 Sequence over S

$f : N \to S$; $\{a_i\}_{i=1}^{\infty}$.
Subsequence: $\{a_{j_i}\}_{i=1}^{\infty}$: $\{j_i\}$ monotonically increasing. (1^k) not subsequence of N.
For topological properties, see topology survey.

8.3.4 Randomized function

For any set S, and set of random variables RV: $f : S \to RV$. RV $f(x)$ independent of $f(y)$ and of previous runs.

8.3.4.1 Functions over vector spaces

See linear algebra survey.

8.3.4.2 Functions defined over convex and affine spaces

See linear algebra survey.

8.3.5 Function families and parameters

Functions with a certain form(ula). An member function over $\{x\}$ actually specified by the parameter t. f(x, t).

8.3.6 Operators

See functional analysis survey.

9 Category theory

9.1 Abstraction

Aka general abstract nonsense. Abstract from sets and relations to categories and morphisms.

9.2 Category

(Class ob(C) of objects, morphisms or arrows hom(C), composition op: $\cdot$) with $\cdot$ identity, associative $\cdot$. Category Eg: Set, $Vect_k$.
Small category: aka CAT: both ob(C) and hom(C) are sets, rather than classes.

9.3 Morphisms

Homomorphism: A structure (identity, inverse elements, and binary ops) preserving funciton f: f(x)=3x preserves addition. Isomorphism: both f and f^{-1}

are homomorphisms. Endomorphism: homomorphism of a mathematical object to itself. Automorphism is both isomorphism and an endomorphism.

9.4 Functors

Structure preserving mapping between categories and their morphisms.

Part IV

Sets with operations

10 Group

10.1 Semigroup, monoid

Semigroup: $< S, + >$: closed under binary operation $+$. **Monoid**: semigroup with identity element e.

10.1.1 Function characteristics

Consider functions on ordered semigroups. Some of these have some notable properties.

10.1.1.1 Subadditivity

$f(a+b) \leq f(a) + f(b)$.

10.2 Group G

Group (G): monoid with inverses. Commutative group. Cayley tables.
No element can have 2 inverses: $a_1^{-1}aa_2^{-1} = a_2^{-1} = a_1^{-1}$. $(ab)^{-1} = b^{-1}a^{-1}$.
Unique solution for ax=b: $x = a^{-1}b$.
For examples Z_n^+ and Z_n^*, see Number Theory survey.

10.2.1 Order of a group

Number of elements in the group, $\phi(G)$.

10.2.2 Subgroups

$H \leq G$. Eg: p prime: $\{\pm 1\} \leq Z_p^*$.

10.2.2.1 Cosets of subgroup

Left coset of subgroup H containing g: gH or g+H; may not be group. Also, right coset of H containing g. Normal subgroup: N for which gN = Ng. Eg: 2Z or 2+Z has 2 cosets: evens and odds.

10.2.2.2 Cardinality

(Lagrange): If $H \leq G : |H|||G|$: Take $a \in G - H$; then $aH \cap H = \phi$; repeat with $a' \in G - H - aH$ etc.. So, if $H < G$, $|H| \leq |G|/2$.
So, this is an easy partial-test to see if H is a group.

10.2.2.3 Quotient/ factor group

G/N: cosets; with Coset product: (aN)(bN) = abNN = abN; eN identity. Eg: Z/nZ isomorphic to $\{0, ..n-1\}, \oplus_n$.
Product group: G*H.

10.2.3 Multiplicative order ord(a) of element a

$ord(a) = argmin_n : a^n = e$. $ord(A)|\phi(G)$.

10.2.4 Cyclic group G generated by a

Every $a \in G$ generates some subgroup of G.
G is cyclic if some generator generates G. Then G is non degenerate. Eg: Z_4; ω in $\omega^n = 1$.

10.2.4.1 Number of generators

If there is a generator g, there are at least $\phi(Z^*_{\phi(G)})$ of them: $Z^*_{\phi(G)}$ excludes all numbers which divide $\phi(G)$; so for any $a \in Z^*_{\phi(G)}$, can't write $(g^a)^b = e$ for any $b < \phi(G)$.

10.2.4.2 Periodic group

Every element has finite order. All finite groups are periodic.

10.3 Group homomorphism

It(a) maps elements of two groups (G,H) : $a(g.h) = a(g).a(h)$. Image a(G). **Kernel** of homomorphism: ker(a) = G elements mapped to 1_H. Isomorphic groups: homomorphism is invertible. ker(a) and a(G) measure closness to homomorphism. ker(a) is a normal subgroup. a(G) isomorphic to G/ker(a).

11 Special groups

11.1 Symmetric group on X

S_X or Sym(X) or S_n is a group of permutations/ bijective functions on X, under composition. Not commutative for $n > 2$. **Transposition** only switches 2 elements. Every permutation f is a product of transpositions. Even and odd permutations. The product is not unique, but oddness is same: Consider number of pairs $i < j$, where $f(j) < f(i)$. Sign of Permutation: Sgn(f) is +1 or -1. Cycle.

11.2 Elliptic curve groups

See topology survey.

11.3 Bilinear groups

Groups with efficiently computable bilinear maps. G_T: target group; g_1, g_2 generators of G_1 and G_2. Bilinear map/ pairing operation: $p : G_1 \times G_2 \to G_T$. Not necessarily 1 to 1.
Bilinearity property: $p(g_1^a, g_2^b) = p(g_1, g_2)^{ab}$; can be seen as bilinear map amongst exponents: $p'(a, b) = ab$. $p(xz, y) = p(z, y)p(x, y)$.
Can efficiently compute bilinear map $Z_p \times Z_p \to Z_p$. [**Find proof**]
No efficient way to make multilinear maps known.

12 Ring

12.1 Ring

$< set, *, + >$: generalizes $< Z, *, + >$. Division ring.

12.1.1 Ideal I of Ring R

Eg: Even numbers, multiples of 3 or 4. **Principle Ideal** is generated by 1 number.

12.1.2 Polynomial ring

The set of polynomials with coefficients taken from a field is a commutative ring. (Z/2Z)(t).

12.2 Field

Division ring with commutative *. Eg: Q, R, C; not Z.
For prime p: GF(p) or Z/pZ or F_p or Z_p: contains both additive, multiplicative subgroup (F^*); Euclid's alg proves inverse for latter. $Z/p^nZ : n > 1$ not a field.
Size of any finite field is a prime power (Find proof); A finite field is a vector space in n dimensions. 2 equisized finite fields are isomorphic.

12.3 Polynomial representation of $GF(p^n)$

Eg: $GF(p^2) : (Z/2Z)(t)/(t^2+1)$ is a finite field. The elements are from the polynomial ring. Operations are performed modulo the polynomial.

12.4 Ordered field

Field which is also an ordered set, with $x + y < x + z$ if $y < z$ and $xy > 0$ if both above 0.
So, $x^2 > 0$; multiplication by +ve (but not -ve) x maintains inequality direction; for $0 < x < y$, $0 < y^{-1} < x^{-1}$.

12.5 Linear algebra over a field

See linear algebr survey.