

Math 455 Spring 2009

David Ross, Department of Mathematics

1 Review of set theory

1.1 Notation

Some set theory notation notation:

$$\in, \{x : \dots\}, \cup, \cap, \subset, \subseteq, \supset, \supseteq, \setminus, \times, \emptyset, \Delta, \mathbb{C}, \mathcal{P}(\dots)$$

- $A \cap B, \quad A \cup B$
- $\cap A, \quad \cup A$
- $(a, b), \quad \langle a, b \rangle$
- $A \times B := \{\langle a, b \rangle \mid a \in A, b \in B\}$
- \exists is shorthand for “there exists”, for example, $\exists x$ such that $x^2 = 2$
- \forall is shorthand for “for all”, for example, $\forall x, x^2 \geq 0$

Proposition 1.1 $\langle x, y \rangle = \langle z, w \rangle$ if and only if $x = z$ and $y = w$

Definition 1.1 A (binary) relation is a set of ordered pairs.

Notation: Let R be a relation.

- We often write xRy instead of $\langle x, y \rangle \in R$
- The *domain* of R is $\text{dom}(R) := \{x \mid \exists y xRy\}$ and the *range* of R is $\text{ran}(R) := \{y \mid \exists x xRy\}$. Note that $R \subset \text{dom}(R) \times \text{ran}(R)$, but that in general the inclusion will be proper.
- $R^{-1} := \{\langle b, a \rangle : \langle a, b \rangle \in R\}$. (Inverse of R .)
- If A a set, then $R \upharpoonright_A := \{\langle a, b \rangle : aRb \text{ and } a \in A\}$ (Restriction of R to A .) (Note: sometimes $R \upharpoonright_A := \{\langle a, b \rangle : aRb \text{ and } a, b \in A\} = R \cap (A \times A)$)
- $R[A] := \text{ran}(R \upharpoonright_A)$ (Image of A under R .)
- If S is another relation, then $R \circ S := \{\langle a, b \rangle : \exists c (aSc \ \& \ cRb)\}$ (Composition of relations.)
- R is *one-to-one* (or *injective*) provided $\forall y \in \text{ran}(R) \exists! x \in \text{dom}(R)(xRy)$

- R is *symmetric* if $\forall a, b(aRb \implies bRa)$
- R is *reflexive* if $\forall a \in \text{dom}(R) aRa$
- R is *transitive* if $\forall a, b, c(aRb \wedge bRc \implies aRc)$
- R is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Fix an equivalence relation R .

- Note $\text{dom}(R) = \text{ran}(R)$.
- For any x , write $[x]_R$ for the *equivalence class* of x (with respect to R), $[x]_R := \{y : xRy\}$. Note that $[x]_R \neq \emptyset$ if and only if $x \in \text{dom}(R)$
- For any x, y either $[x]_R = [y]_R$ or $[x]_R \cap [y]_R = \emptyset$ (Why?) It follows that $\text{dom}(R)$ can be written as the union of a set of pairwise disjoint sets, $\text{dom}(R) = \{[x]_R : x \in \text{dom}(R)\}$.
- If X is any set, a *partition* of X is a set P of sets such that (a) $X = \cup P$ and (b) $\forall x, y \in P(x = y \vee x \cap y = \emptyset)$. We say that P *partitions* X . If P and R are as in the last paragraph, we say that P is the partition *induced* or *generated* by the equivalence relation R , and write X/R (or $X \bmod R$) for the set of equivalence classes (which is of course the same as the set of elements of the partition).
- Conversely, suppose that P is a partition of a set X . We can define a relation R on X by xRy if and only if x and y are in the same element of P ; that is, $R := \{\langle x, y \rangle \in X^2 : \exists w \in P(x, y \in w)\}$ (We say that R is the equivalence relation *induced* or *generated* by P .)

Definition 1.2 A function is a relation F such that $\forall a \in \text{dom}(F) \exists! b (aFb)$

- For functions F we usually write $F(a) = b$ instead of aFb . If $A = \text{dom}(F)$ and $\text{ran}(F) \subseteq B$ then we often write $F A \rightarrow B$
- Note a relation F is *one-to-one* if and only if F^{-1} is a function.
- In particular, if F is a function then F^{-1} respects all Boolean operations:

$$\begin{aligned} - F^{-1}[\cup \mathcal{A}] &= \cup \{F^{-1}[A] : A \in \mathcal{A}\} \\ - F^{-1}[\cap \mathcal{A}] &= \cap \{F^{-1}[A] : A \in \mathcal{A}\} \\ - F^{-1}[A] - F^{-1}[B] &= F^{-1}[A - B] \end{aligned}$$

- If F, G are functions, then $F \circ G$ is a function, and $(F \circ G)(x) = F(G(x))$ for every $x \in \text{dom}(G) = \text{dom}(F \circ G)$

Definition 1.3 The n -tuple $\langle a_1, \dots, a_n \rangle$ is defined by induction:

$$\langle a_1 \rangle := a_1; \quad \langle a_1, a_2, \dots, a_{n+1} \rangle := \langle \langle a_1, a_2, \dots, a_n \rangle, a_{n+1} \rangle$$

- Note that this uses our previous definition for ordered pair, and agrees with it when $n = 1$
- We can now define an *n -ary relation* to be a set of ordered n -tuples.
- If A_1, \dots, A_n are sets then $A_1 \times A_2 \times \dots \times A_n$ is defined to be the set of n -tuples $\langle a_1, \dots, a_n \rangle$ such that $a_i \in A_i$ for all i . Equivalently, $A_1 \times A_2 \times \dots \times A_n := (\dots((A_1 \times A_2) \times A_3) \times \dots) \times A_n$
- We usually denote the n -fold Cartesian product of one fixed set A by $A^n := A \times A \times \dots \times A$ (n times)
- An ordered n -tuple is also an ordered pair; it follows that an n -ary relation is also a binary relation. Call an n -ary relation f an *n -ary function* if f is a function when viewed as a binary relation; $\text{dom}(f)$ and $\text{ran}(f)$ are defined accordingly. We often write $f(a_1, \dots, a_n)$ for $f(\langle a_1, \dots, a_n \rangle)$

Definition 1.4 If A, B are sets then ${}^A B$ is the set of functions from A to B .

Note that any $f: A \rightarrow B$ is a subset of $A \times B$, so ${}^A B$ is a subset of $\mathcal{P}(A \times B)$.

We can view ${}^A B$ as a kind of infinite Cartesian product. For each $a \in A$ let $B_a = B$; then ${}^A B$ corresponds to our intuition for the infinite product $\prod_{a \in A} B_a$.

More generally, let A be a set, and B a function on A . (That is, $B(a)$ can vary with A , as opposed to the constant B we just discussed.) Then $\prod_{a \in A} B(a)$ is the set of all functions f with domain A satisfying $f(a) \in B(a)$ for every $a \in A$. (Note that $\prod_{a \in A} B(a)$ will be a subset of ${}^A[\cup \text{ran}(B)]$). Other notations: $\prod_{a \in A} B_a$, $\bigotimes_{a \in A} B(a)$, etc. A is called the *index set* for the product.

1.2 Cardinality

$\mathbb{N} = \omega = \aleph_0 =$ the *natural numbers* = $\{0, 1, 2, 3, \dots\}$

We usually identify a natural number with the set of its predecessors: $n = \{0, 1, 2, \dots, n - 1\}$ In particular, $0 = \emptyset$.

Definition 1.5 *A is equinumerous with B provided there is a bijection from A onto B.*

Other, equivalent notation/terminology for “A is equinumerous with B”:

- a. *A and B have the same cardinality*
- b. $A \approx B$
- c. $\text{card}(A) = \text{card}(B)$

Theorem 1.1 *For any sets A, B, and C:*

1. $A \approx A$
2. $A \approx B \implies B \approx A$
3. $A \approx B \ \& \ B \approx C \implies A \approx C$

Definition 1.6 *A has no greater cardinality than B (or $\text{card}(A) \leq \text{card}(B)$, or $A \preceq B$) provided there is an injection from A into B.*

Theorem 1.2 *For any nonempty sets A and B the following are equivalent:*

1. $\text{card}(A) \leq \text{card}(B)$
2. *For some $C \subseteq B$, $\text{card}(A) = \text{card}(C)$*
3. *There is a function g from B onto A.*

Theorem 1.3 (Cantor-Schroder-Bernstein) *If $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(A)$ then $\text{card}(A) = \text{card}(B)$*

Theorem 1.4 (Cantor) *For any set A , $\text{card}(A) \neq \text{card}(\mathcal{P}(A))$ (in fact, $\text{card}(A) < \text{card}(\mathcal{P}(A))$)*

Proof: Let g be any 1 – 1 function from A into $\mathcal{P}(A)$. Put $B = \{x \in A : x \notin g(x)\}$ Claim: $B \notin \text{range}(g)$. To see this, let $x_0 \in A$, and consider 2 cases: (i) $x_0 \in g(x_0)$; then $x_0 \notin B$, so $B \neq g(x_0)$. (ii) $x_0 \notin g(x_0)$; then $x_0 \in B$, so $B \neq g(x_0)$. Either way, $B \neq g(x_0)$. Since x_0 was arbitrary in A , $B \notin \text{range}(g)$. Since g was arbitrary, $A \not\approx \mathcal{P}(A)$. (Note that $a \mapsto \{a\}$ is an injection from A into $\mathcal{P}(A)$, so $\text{card}(A) \leq \text{card}(\mathcal{P}(A))$.)

Proposition 1.2 *For every set A , $\mathcal{P}(A) \approx {}^A 2$*

Proof: Define $f : \mathcal{P} \rightarrow {}^A 2$ by $f(\alpha) = \chi_\alpha$, where $\chi_\alpha(x) = 1$ if $x \in \alpha$, $= 0$ otherwise (i.e., χ_α is the characteristic function of the set α). Claim: f is a bijection. 1 – 1: If $\alpha \neq \beta$ are in $\mathcal{P}(A)$ then WOLOG there is some $n \in \beta - \alpha$. Then $\chi_\alpha(n) = 0, \chi_\beta(n) = 1$, so $f(\alpha) \neq f(\beta)$. Onto: If $\phi \in {}^A 2$ then put $\alpha = \phi^{-1}(1)$. Then $\chi_\alpha(n) = 1 \iff n \in \alpha \iff \phi(n) = 1$, so $f(\alpha) = \phi$.

Theorem 1.5 Suppose $A \neq \emptyset$. The following are equivalent:

1. $\exists m \in \omega \ A \approx m$
2. $A \preceq \omega$ but $A \not\approx \omega$
3. It is not the case that $\exists B \subsetneq A \ A \approx B$
4. There exists an injection $f : A \rightarrow m$ for some $m \in \omega$
5. There exists a surjection $g : m \rightarrow A$ for some $m \in \omega$

Definition 1.7 Call a set A satisfying any of the conditions of this theorem *finite*

Definition 1.8 A is *countable* (or *enumerable* or *denumerable*) if either A is finite or $A \approx \omega$.

Theorem 1.6 Suppose $A \neq \emptyset$. The following are equivalent:

1. A is countable
2. $A \preceq \omega$
3. There is a surjection f from ω onto A

Remark: We will call a set A *countably infinite* if it is countable and infinite. This is of course, just another way of saying that $A \approx \omega$.

An alternate approach to countability:

Definition 1.9 If Σ is any set (which we think of as a set of “letters”, let Σ^* be the set of finite “words” on Σ ; formally, $\Sigma^* := \bigcup_{n < \omega} {}^n\Sigma$

Theorem 1.7 If Σ is countable then so is Σ^*

Proof: Without loss of generality $\Sigma \subseteq \omega - \{0\}$. Define $\phi : \Sigma^* \rightarrow \omega$ by $\phi(\tau) = p_0^{\tau(0)} p_1^{\tau(1)} \cdots p_{n-1}^{\tau(n-1)}$, where $n = \text{domain}(\tau)$ and p_0, p_1, \dots enumerates the prime numbers. It is easy to see that ϕ is one-to-one, and that suffices.

Corollary 1.1 \mathbb{Q} is countable

Proof: Every rational can be written as a word on the finite alphabet $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, /, -\}$; eg, $\frac{-37}{4}$ is the 5 character word “-37/4”.

Corollary 1.2 *if A and B are countable then $A \times B$ is countable*

Proof: Every pair in $A \times B$ can be written as a word on the alphabet $A \cup B \cup \{(\,,\,)\}$ (note the comma in the last set).

Note (exercise!) that this can be easily extended to a finite product.

Theorem 1.8 *A countable union of countable sets is countable.*

Theorem 1.9 *If A is infinite then A has a countably infinite subset*

1.3 Closures

Let X be a set, $f : X^n \rightarrow X$, and $A \subseteq X$. Say that A is *closed under f* provided $f[A^n] \subseteq A$, that is, $\forall a_1, \dots, a_n \in A, f(a_1, \dots, a_n) \in A$. If \mathcal{F} is a *set* of such functions (possibly of different arities), say that A is *closed under \mathcal{F}* provided that for every $f \in \mathcal{F}$, A is closed under f .

Theorem 1.10 *If X a set, \mathcal{F} a set of functions such that for every $f \in \mathcal{F}$, $\text{domain}(f) \subseteq X^n$ (where $n = \text{the arity of } f$), and $A \subseteq X$, then there is a set $B \subseteq X$, the closure of A under \mathcal{F} , such that:*

1. B is closed under \mathcal{F} ;
2. $A \subseteq B$; and
3. $\forall \hat{B}, B \subseteq \hat{B} \subseteq X \wedge \hat{B}$ closed under $\mathcal{F} \implies \hat{B} = B \vee \hat{B} = X$
(in other words, B is the minimal superset of A closed under \mathcal{F}).

Example 1.1 *Let Σ be the countable alphabet*

$$\Sigma = \{ (,), \neg, \wedge, \vee, \rightarrow, \leftarrow, \leftrightarrow, A_0, A_1, A_2, \dots, A_n, \dots \}$$

and let $X = \Sigma^*$, as usual the set of finite words on Σ . Define functions f, g, h, γ, ρ by:

$$f(x) = "(\neg x)"$$

$$g(x, y) = "(x \wedge y)"$$

$$h(x, y) = "(x \vee y)"$$

$$\gamma(x, y) = "(x \rightarrow y)"$$

$$\rho(x, y) = "(x \leftrightarrow y)"$$

Then the closure of $A = \{A_0, A_1, \dots, A_n, \dots\}$ under $\mathcal{F} = \{f, g, h, \gamma, \rho\}$ is the set of Well-Formed Formulas (or WFFs) of propositional logic. (Write out some examples!) We will see these again later.

1.4 Orders, ordinals, cardinals

We will occasionally have occasion to use the *Axiom of Choice* (AC). One common form of this axiom is:

Zorn's Lemma: Let \mathcal{A} be a set, suppose \mathcal{A} is closed under unions of chains. Then \mathcal{A} contains a maximal element.

(Here a *chain* is a set C such that $\forall x, y \in C, x \subseteq y \vee y \subseteq x$. The hypothesis on \mathcal{A} is that $\forall C \subseteq \mathcal{A}$, if C is a chain then $\bigcup C \in \mathcal{A}$. A *maximal element* in this setting is an $M \in \mathcal{A}$ such that $\forall A \in \mathcal{A}$, if $M \subseteq A$ then $M = A$.)

Zorn's Lemma is not always the easiest form of AC to use. For the next, we recall a couple of definitions.

Definition 1.10 A binary relation \leq is a partial order on A provided \leq is reflexive, antisymmetric, and transitive. \leq is a linear order provided in addition any two elements are comparable, that is, $\forall x, y \in A, x \leq y \vee y \leq x$. (In other words, trichotomy holds.) A partial order \leq on A is well-founded provided every nonempty subset of A has a minimal element. A well-founded partial order is a well order.

Note that a nonempty subset in a well-founded relation might have several minimal elements, but in a linear order every minimal element is a *minimum* element.

Another version of AC is the

Well-Ordering Principle: Every set can be well-ordered.

To convince yourself that this axiom is ludicrous, note that it means that there is a well-ordering of \mathbb{R} (not of course the usual ordering). However, it is equivalent to Zorn's Lemma, and for the remainder of the course we will assume it is true (unless we specify otherwise).

Now, consider the natural numbers again:

$$\omega = \{0, 1, 2, \dots, n \dots\}$$

As we defined them before, each natural number is an element of its successor, in fact of *all* its successors, and in fact the usual ordering on ω is just \in . Moreover, the set is well-ordered under this ordering. Everything I just said remains true if we consider $\omega + 1 := \omega; \omega$ in place of ω . This motivates the following definition:

Definition 1.11 An ordinal is a set α , well-ordered by \in , such that whenever $x \in y \in \alpha$, $x \in \alpha$.

Intuitively, the ordinals line up ‘forever’, and each ordinal is the set of all earlier ones.

The first important property of ordinals is that there are ‘canonical’ well-ordered sets:

Theorem 1.11 Every well-ordered set A is order isomorphic to an ordinal α

By *order-isomorphic* I mean that there is a bijection f from A onto α , and that $x < y \iff f(x) < f(y)$ for all $x, y \in A$. In fact, the isomorphism f is easily defined recursively by $f(x) := \{f(y) : y < x, y \in A\}$ for $x \in A$. While I won’t give the proof here that this f is an order isomorphism, you should compute f for the first few elements of A and convince yourself that it will work.

Theorem 1.12 (*Trichotomy for ordinals*) If α, β are ordinals then exactly one of $\alpha < \beta$, $\alpha = \beta$, $\alpha > \beta$ hold (where $<$ is \in).

Remark: The proof is surprisingly hard, so is omitted.

Definition 1.12 If A is a set, then $\text{card}(A)$ is defined to be the least ordinal α such that $\alpha \approx A$. An ordinal α is a cardinal number provided $\alpha = \text{card}(\alpha)$

Remark: The fact that $\text{card}(A)$ exists for every A is a consequence of choice: well-order A , find an isomorphic ordinal α' using the theorem above, then find the least $\alpha \in \alpha'$ such that $\alpha \approx \alpha'$ (which we can do since α' is well-ordered). In fact, the statement “Every set has a cardinality” is *equivalent* to choice; you should be able to see why this is so.