MHF 3202, Dr. Block, Course Notes, 2-23-2020

Notes for Chapter 1

1. In this class, we adopt an informal approach to set theory. A set is a collection of things called elements. We use the notation $x \in A$ to denote that x is an element of the set A. We use the notation $x \notin A$ to denote that x is not an element of the set A. Two sets are equal if and only if they contain exactly the same elements. A set S may be either finite or infinite. If S is a finite set, the **cardinality** of S denoted $|S|$ is the number of elements in $|S|$.

2. The unique set with cardinality zero is called the empty set and denoted ϕ.

3. We let $\mathbb{R}$ denote the set of real numbers, $\mathbb{Q}$ the set of rational numbers, $\mathbb{Z}$ the set of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, and $\mathbb{N}$ the set of positive integers, $\mathbb{N} = \{1, 2, 3, \ldots\}$.

4. We can in general form a new set from an existing set A by taking all elements of A which satisify a given property. Forming a new set in this way is called **specification**.

   For example, the set of rational numbers is given by

   $$\mathbb{Q} = \{x \in \mathbb{R} : x = \frac{p}{q} \text{ for some } p, q \in \mathbb{Z} \text{ with } q \neq 0\}.$$

5. Suppose that A and B are sets. We let $A \times B$ denote the set of ordered pairs (a, b) such that $a \in A$ and $b \in B$. Two ordered pairs (c, d) and (v, w) are equal if and only if $c = v$ and $d = w$. The set $A \times B$ is called the **Cartesian product** of A and B.

6. More generally, if n is a positive integer and $A_1, A_2, \ldots A_n$ are sets, we define the Cartesian product of these sets by

   $$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_1 \in A, x_2 \in A_2, \ldots, x_n \in A_n\}.$$

   The expression $(x_1, x_2, \ldots, x_n)$ is called an ordered n-tuple. Two ordered n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are equal if and only if $x_i = y_i$ for each $i = 1, 2, \ldots, n$. Note the meaning of $\ldots$ (dots).

7. If A is a set and n is a positive integer we define the **Cartesian power** A^n by
$$A^n = A_1 \times A_2 \times \cdots \times A_n,$$
where $A_i = A$ for each $i = 1, 2, \ldots, n$.

8. Suppose that A and B are sets. We say that A is a **subset** of B, denoted $A \subseteq B$, if and only if every element of A is also an element of B. We note that two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

9. Note that for any set A, we have $\phi \subseteq A$.

10. Suppose that A and B are sets. We assume that there exist sets $A \cap B$, $A \cup B$, and $A - B$ given by

    $x \in A \cap B$ if and only if $x \in A$ and $x \in B$,

    $x \in A \cup B$ if and only if $x \in A$ or $x \in B$,

    $x \in A - B$ if and only if $x \in A$ and $x \notin B$.

    These sets are called the **intersection, union**, and **difference** of the sets A and B. The notation $A \setminus B$ is often used instead of $A - B$.

11. If A is a set, we assume that there exists a unique set S such that $x \in S$ if and only if $x \subseteq A$. This set is called the **power set** of A and is denoted by $\mathscr{P}(A)$. So $x \in \mathscr{P}(A)$ if and only if $x \subseteq A$. Note that if a finite set A has n elements, then $\mathscr{P}(A)$ is a finite set which has 2^n elements.

12. Suppose that S is a set, and for each $s \in S$, a set A_s is defined. We assume that there are sets denoted by $\bigcup_{s \in S} A_s$ and $\bigcap_{s \in S} A_s$ such that $x \in \bigcup_{s \in S} A_s$ if and only if there exists $s \in S$ with $x \in A_s$, and $x \in \bigcap_{s \in S} A_s$ if and only if for every $s \in S$ we have $x \in A_s$.

    The set S is called an **index set**, the family of sets A_s is called an **indexed family of sets**, the set $\bigcup_{s \in S} A_s$ is called the **union of the indexed family of sets**, and the set $\bigcap_{s \in S} A_s$ is called the **intersection of the indexed family of sets**.

    If $S = \{1, 2, \ldots, n\}$, instead of $\bigcup_{s \in S} A_s$ we often write $\bigcup_{i=1}^{n} A_i$ or $A_1 \cup A_2 \cup \cdots \cup A_n$.

If $S = \mathbb{N}$, instead of $\bigcup_{s \in S} A_s$ we often use the notation $\bigcup_{i=1}^{\infty} A_i$ or $A_1 \cup A_2 \cup \ldots$.

The same is true for $\bigcap_{s \in S} A_s$.

13. Sometimes, we restrict attention to subsets of some understood larger set, which we call a **universal set** or universe. If a universal set U is understood, we may define the complement of a set B. (If it is not clear what the universe is we say the complement of B in U.) In our text, the complement of B is denoted by $\overline{B}$ and given by $\overline{B} = U - B$.

14. We can not just assume that anything is a set without the possibility of running into problems. See **Russell's paradox** on page 32 of the text. On the other hand, we may form new sets from existing sets using specification, unions, intersections, power sets, and Cartesian products without running into problems.

15. Before we begin to prove some results, we will accept some things as facts. We will accept the basic properties of real numbers (see the link on the course website). Also,

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

In addition, we will accept the following as facts.

16. **Fact.** Any nonempty subset of $\mathbb{N}$ has a smallest element.

17. **Fact.** Any finite nonempty subset of $\mathbb{R}$ has a largest element and a smallest element.

18. **Fact and Notation.** If $x \in \mathbb{R}$ and $x \geq 0$, then there is a unique $y \in \mathbb{R}$ such that $y \geq 0$ and $y^2 = x$. This number y is denoted by $\sqrt{x}$.

19. **Fact.** If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$, $-a \in \mathbb{Z}, ab \in \mathbb{Z}$, and $a - b \in \mathbb{Z}$.

Notes for Chapter 2

20. A **statement** is a sentence that is either definitely true or definitely false. An **open sentence** is a sentence whose truth depends on the value of one or more variables. If P and Q are statements or open sentences, we can form three new expressions:

    $P \wedge Q$ (and)

    $P \vee Q$ (or)

    $\sim P$ (negation)

    See the truth tables for these expressions on page 15 of the text.

21. We can also form more compicated logical expressions such as

$$(P \wedge Q) \vee (\sim P \wedge \sim Q)$$

    and construct truth tables.

22. We say that two logical expressions P and Q are logically equivalent if and only if P is true whenever Q is true, and P is false whenever Q is false. See the laws on page 52 of the text.

23. A logical expressions which is always true is called a tautology. A logical expressions which is always false is called a contradiction.

24. If P and Q are statements, we can also form the two new statements:

    $P \Rightarrow Q$ (implies) (conditional statement)

    $P \Leftrightarrow Q$ (is equivalent to) (biconditional statement).

    See the truth tables for these statements on pages 43 and 47 of the text.

25. Note that $P \Rightarrow Q$ is equivalent to $\sim P \vee Q$, and $\sim (P \Rightarrow Q)$ is equivalent to $P \wedge \sim Q$.

26. Also, $P \vee Q$ is equivalent to $\sim P \Rightarrow Q$. This equivalence is often used to prove a statement of the form $P \vee Q$.

27. Contrapositive Law.

    $P \Rightarrow Q$ is equivalent to $\sim Q \Rightarrow \sim P$.

28. If C is a contradiction, then $(P \wedge \sim Q) \Rightarrow C$ is equivalent to $P \Rightarrow Q$. This fact, is the basis for proof by contradiction, which we will discuss later.

29. Here are some ways to express the statement $P \Rightarrow Q$:

    If P then Q.

    P implies Q.

    P is a sufficient condition for Q.

    Q is a necessary condition for P.

    P only if Q.

30. Here are some ways to express the statement $P \Leftrightarrow Q$:

    P if and only if Q.

    Q is a necessary and sufficient condition for P.

31. The converse of a statement $P \Rightarrow Q$ is the statement $Q \Rightarrow P$. The converse of a true statement need not be true.

32. We introduce the universal quantifier $\forall$ and the existential quantifier $\exists$. A statement of the form $\forall x$, $P(x)$ means that for all x in the universe $P(x)$ is true. A statement of the form $\forall x \in B$, $P(x)$ means that for all x in the set B, $P(x)$ is true. A statement of the form $\exists x$, $P(x)$ means that there exists x in the universe such that $P(x)$ is true. A statement of the form $\exists x \in B$, $P(x)$ means that there exists x in the set B with $P(x)$ true. In mathematics the words "for some x" mean "there exists x".

33. Quantifier Negation laws:

    $\sim (\exists x \in A,\, P(x))$ is equivalent to $\forall x \in A, \sim P(x)$.

    $\sim (\forall x \in A,\, P(x))$ is equivalent to $\exists x \in A, \sim P(x)$.

34. Many mathematical statements are in the form

$$\forall x \in A,\, (P(x) \Rightarrow Q(x)).$$

    Sometimes, this will be shortened to $P(x) \Rightarrow Q(x)$. When this is done, the $\forall x \in A$ is understood.

To prove a statement of this form, we begin the proof with "Suppose $x \in A$ and $P(x)$." Then we prove $Q(x)$. Sometimes the "$x \in A$" is understood but not explicitly stated.

35. Here are three rules of inference that we sometimes use.

    (modus ponens) If P and $P \Rightarrow Q$ are both true, we can conclude that Q is true.

    (modus tollens) If Q is false and $P \Rightarrow Q$ is true, we can conclude that P is false.

    (elimination) If $P \vee Q$ is true and P is false, then Q is true.

Notes for Chapter 3

36. We may later use the following. We will accept this without proof.

    Theorem (Binomial Theorem). Suppose that $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\, b^k,$$

    where

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Notes for Chapter 4

37. Here are some important terms that are use in mathematics.

    A **theorem** is a mathematical statement that has been verified to be true.

    A **proof** of a theorem is a written verification that shows that the theorem is unequivocally true.

    Sometimes in mathematical material the word **proposition** is used in place of the word theorem. The most significant results are called theorems, and the other results are called proposition.

    A **lemma** is a theorem whose main purpose is to prove another theorem.

    A **corollary** is a result which follows easily from another theorem.

38. To prove a statement of the form $P \Rightarrow Q$ with a direct proof:

    Begin the proof with "Suppose P"

    End the proof with "Therefore Q."

39. **Definition.** Suppose a and b are integers. We say that a **divides** b, written $a|b$ if and only if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

40. **Proposition.** Suppose that $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(b+c)$.

41. **Proposition.** Suppose that $a, b, c \in \mathbb{Z}$. If $a|b$, then $a|(bc)$.

42. **Proposition.** Suppose that n and k are positive integers and $k|n$. Then $k \in \{1, 2, \ldots, n\}$.

43. **Theorem (The Division Algorithm).** If $a, b \in \mathbb{Z}$ and $b > 0$, then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

44. **Definition.** An integer n is **even** if and only if n=2a for some $a \in \mathbb{Z}$. An integer n is **odd** if and only if n=2a+1 for some $a \in \mathbb{Z}$.

45. **Remark.** It is a common convention in mathematics to use "if" instead "if and only if" in definitions. With this convention it is understood that the word "if" means "if and only if". This convention is used in the text, but not in these notes. On the other hand in mathematical theorems, this convention is never used. In theorems, "if" always has a different meaning than "if and only if".

46. **Proposition.** An integer n is either even or odd, but not both even and odd.

47. **Definition.** Two integers have the **same parity** if and only if they are both even or both odd. Two integers have the **opposite parity** if and only if they do not have the same parity.

48. **Definition.** Suppose that n is an integer with $n \geq 2$. We say that n is **composite** if and only if there exists a divisor b of n with $1 < b < n$. We say that n is **prime** if and only if n is not composite.

49. **Remark.** Suppose that n is an integer with $n \geq 2$. Then n is prime if and only if n has exactly two positive divisors, 1 and n.

50. **Definition.** Suppose that a and b are integers, not both zero. The **greatest common divisor** of a and b, denoted $gcd(a, b)$, is the largest integer that divides both a and b.

51. **Definition.** Suppose that a and b are non-zero integers. The **least common multiple** of a and b, denoted $lcm(a, b)$, is the smallest positive integer that is a multiple of both a and b.

52. **Proposition.** If $a, b, c \in \mathbb{N}$, then $lcm(ca, cb) = c \cdot lcm(a, b)$.

Notes for Chapter 5

53. To prove a statement of the form $P \Rightarrow Q$ by contrapositive, begin the proof with: "Suppose $\sim Q$." End the proof with: "Therefore $\sim P$.

54. **Definition.** Let $m \geq 1$ be an integer, and let x and y be integers. We say that x is congruent to y modulo m if and only if m divides $x - y$. We use the notation,

$$x \equiv y \,(\mathrm{mod}\, m).$$

55. **Definition.** Suppose that $a, n, r \in \mathbb{Z}$, $n > 0$, and $0 \leq r < n$. If there is an integer q with $a = qn + r$, we say that a **has remainder** r **when divided by** n.

Notes for Chapter 6

56. To prove a statement P with a proof by contradiction: Begin the proof with "Suppose $\sim P$."

    End the proof by proving a contradiction (a statement of the form $R \wedge \sim R$).

    Sometimes either R or $\sim R$ is something known by a previous result.

    This method is valid because if C is a contradiction, then $(\sim P \Rightarrow C)$ is equivalent to P.

57. Here is one way prove a statement of the form $P \Rightarrow Q$ with a proof by contradiction: Begin the proof with "Suppose P."

    Next say: "Proceeding by contradiction, suppose $\sim Q$."

    End the proof by proving a contradiction (a statement of the form $R \wedge \sim R$).

58. Here is a slight variation in the wording (as suggested in the text). To prove a statement of the form $P \Rightarrow Q$ with a proof by contradiction:

    Begin the proof with "For the sake of contradiction, suppose P and $\sim Q$."

    End the proof by proving a contradiction (a statement of the form $R \wedge \sim R$).

    This method of proof is valid because if C is a contradiction, then $(P \wedge \sim Q) \Rightarrow C$ is equivalent to $P \Rightarrow Q$.

59. **Proposition.** Suppose that n is a positive integer and a is an integer. Then there exists a unique $r \in \{0, 1, \ldots, n-1\}$ such that

$$a \equiv r \pmod{n}.$$

60. **Fact.** If q is a positive rational number, then there exist positive integers a and b such that $q = \frac{a}{b}$ and the greatest common divisor of a and b is 1. (Informally we say the fraction is reduced.)

61. **Proposition.** Suppose that $n \geq 2$ is an integer. Then n has a prime divisor.

62. If a case by case argument is used in a proof by contradiction, a contradiction must be obtained in each case.

63. **Proposition.** Suppose that $x, y, z \in \mathbb{Z}$ and $x^2 + y^2 = 3z^2$. Then $x = y = z = 0$.

Notes for Chapter 7

64. To prove a statement of the form $P \Leftrightarrow Q$ the most common way is to prove that both $P \Rightarrow Q$ and $Q \Rightarrow P$. It is best to put each of these statements with the proof in a separate paragraph. We sometimes call the two statements the two directions of the proof. Each direction may be proved by direct proof, contrapositive proof, or proof by contradiction. You do not have to use the same method for each direction.

65. To prove a statement of the form $\exists x \in A$, $P(x)$:

    Begin the proof by exhibiting a particular $x_0 \in A$.

    End the proof by proving that $P(x_0)$ holds.

66. To prove a statement of this form: "There exists a unique $x \in A$ such that $P(x)$ holds".

    Begin the proof of existence by exhibiting a particular $x_0 \in A$.

    End the proof of existence by proving that $P(x_0)$ holds.

    Prove uniqueness as follows:

    Suppose $x \in A$ and $P(x)$ holds. Then prove that $x = x_0$.

67. An alternate way to prove uniqueness is: Suppose that $x_1 \in A$, $x_2 \in A$ and both $P(x_1)$ and $P(x_2)$ hold. Then prove that $x_1 = x_2$.

68. Here are some ways to prove a statement of the form $P \vee Q$.

    * Suppose $\sim P$ and prove Q.

    * Suppose $\sim Q$ and prove P.

    * Proceed by contradiction.

    * Make cases and deal with each case separately. When you do this the cases must cover every possibility. Here is one example: Suppose that x is an integer.

    Case 1. x is even.

    Case 2. x is odd.

69. **Proposition.** Suppose that a and b are positive integers. Then there exist integers k and ℓ such that

$$gcd(a, b) = ak + b\ell.$$

Notes for Chapter 8

70. To prove that $a \in \{x : P(x)\}$, prove that $P(a)$ is true. To prove that $a \in \{x \in S : P(x)\}$, prove that $a \in S$ and prove that $P(a)$ is true.

71. Suppose that A and B are sets. The statement $A \subseteq B$ is equivalent to the conditional statement:

    "If $a \in A$, then $a \in B$."

    So any of the methods for proving conditional statements may be used.

72. One common method to prove that two sets are equal is to prove that each of the sets is a subset of the other.

73. **Definition.** A natural number x is perfect if and only if the sum of all of the positive divisor of x which are less than x is equal to x.

74. **Theorem.** If $A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{and } 2^n - 1 \text{ is prime}\}$ and $P = \{p \in \mathbb{N} : p \text{ is perfect}\}$, then $A \subseteq P$.

75. **Definition.** A prime number of the form $(2^n - 1)$ for some $n \in \mathbb{N}$ is called a **Mersenne prime**.

76. **Theorem.** If $A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{and } 2^n - 1 \text{ is prime}\}$ and $E = \{p \in \mathbb{N} : p \text{ is perfect and even}\}$, then $A = E$.

Notes for Chapter 9

77. To disprove a statement P, prove $\sim P$.

78. The most common method used to disprove a universal statement, is to give a counterexample. Note that the negation of the statement

$$\forall x \in S, P(x)$$

is the statement

$$\exists x \in S, \sim P(x).$$

Recall item 57 above.

79. To disprove a statement with contradiction: Suppose the statement is true and then deduce a contradiction.

Notes for Chapter 10

80. **Theorem (Mathematical Induction).** Suppose that j is a non-negative integer. Suppose that for each integer $n \geq j$ we have an associated statement S_n. Suppose that

1. S_j is true and

2. For all $k \in \mathbb{Z}$ with $k \geq j$, if S_k is true, then S_{k+1} is also true.

Then for all $n \in \mathbb{Z}$ with $n \geq j$ the statement S_n is true.

81. **Theorem (Mathematical Induction, Strong Form).** Suppose that j is a non-negative integer. Suppose that for each integer $n \geq j$ we have an associated statement S_n. Suppose that

1. S_j is true and

2. For all $k \in \mathbb{Z}$ with $k \geq j$ if each of the statements $S_j, S_{j+1}, \ldots S_k$ are true, then the statement S_{k+1} is also true.

Then for all $n \in \mathbb{Z}$ with $n \geq j$ the statement S_n is true.

82. A method of proof similar to mathematical induction is proof by smallest counterexample. Suppose that j is a non-negative integer. Suppose that for each integer $n \geq j$ we have an associated statement S_n. If the statements S_n are not all true, then there is a smallest

k such that S_k is false. This can sometimes be used to obtain a contradiction.

Notes for Chapter 11

83. **Definition and Notation.** A **relation** on a set A is a subset R of the Cartesian product $A \times A$. We often use the notation xRy instead of $(x, y) \in R$.

84. **Definition.** Suppose that R is a relation on a set A.

    R is **reflexive** if and only if for all $\forall x \in A, xRx$.

    R is **symmetric** if and only if $\forall x, y \in A, (xRy \Rightarrow yRx)$.

    R is **transitive** if and only if $\forall x, y, z \in A, ((xRy \wedge yRz) \Rightarrow xRz)$.

85. **Definition.** Suppose that R is a relation on a set A. We say that R is an **equivalence relation** on A if and only if R is reflexive, transitive, and symmetric.

86. **Definition.** Suppose that R is an equivalence relation on A. Suppose that $x \in A$. The **equivalence class** of x denoted $[x]$ is given by

$$[x] = \{y \in A : xRy\}.$$

    We let A/R (in words, A modulo R) denote the set of equivalence classes.

87. **Theorem.** Suppose that R is an equivalence relation on A. Suppose that $x, y \in A$. Then xRy if and only if $[x] = [y]$.

88. **Definition.** Suppose that D and E are sets. We say that D and E are disjoint if and only if $D \cap E = \phi$.

89. **Definition.** Suppose that A is a set and $\mathcal{F} \subseteq \mathscr{P}(A)$. We say that $\mathcal{F}$ is **pairwise disjoint** iff every pair of distinct elements of $\mathcal{F}$ are disjoint. We say that $\mathcal{F}$ is a **partition** of A if and only if $\mathcal{F}$ is pairwise disjoint, $\phi \notin \mathcal{F}$, and the union of all of the sets which are elements of $\mathcal{F}$ is equal to A.

90. **Propostion.** Suppose that A is a set, and $\mathcal{F} \subseteq \mathscr{P}(A)$ such that $\phi \notin \mathcal{F}$. Then $\mathcal{F}$ is a partition of A if and only if for every $x \in A$ there is a unique $B \in \mathcal{F}$ such that $x \in B$.

91. **Theorem.** Suppose that R is an equivalence relation on A. Then A/R is a partition of A.

92. **Theorem.** Suppose that A is a set, and $\mathcal{F}$ is a partition of A. Then there is an equivalence relation R on A such that $A/R = \mathcal{F}$.

93. **Theorem.** Let $m \geq 2$ be an integer, and let C_m denote the set of ordered pairs $(x, y) \in (\mathbb{Z} \times \mathbb{Z})$ such that

$$x \equiv y \,(\mathrm{mod}\, m).$$

Then C_m is an equivalence relation on $\mathbb{Z}$. Moreover, there are exactly m distinct equivalence classes given by $[0], [1], \ldots, [m-1]$.

94. **Definition.** The set of equivalence classes for the relation C_m in the previous theorem is denoted by $\mathbb{Z}_m$. This set is sometimes called the integers modulo m.

95. **Theorem.** Let $m \geq 2$ be an integer. Suppose that $a, b, c, d \in \mathbb{Z}$ satisfy

$$a \equiv c \,(\mathrm{mod}\, m) \text{ and } b \equiv d \,(\mathrm{mod}\, m).$$

Then $a + b \equiv c + d \,(\mathrm{mod}\, m)$ and $ab \equiv cd \,(\mathrm{mod}\, m)$.

96. **Definition and Remark.** We can define two operations, which we call addition and multiplication, on the set $\mathbb{Z}_m$ by

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [a \cdot b].$$

This is well-defined in light of the previous theorem.

Notes for Chapter 12

97. **Definition.** We say that f is a relation from A to B if and only if $f \subseteq (A \times B)$.

98. **Definition.** Suppose that f is a relation from A to B. We say that f is a **function** from A to B if and only if for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$. We use the notation $f : A \to B$ to indicate that f is a function from A to B. Also, if $a \in A$, we let $f(a)$ denote the unique $b \in B$ such that $(a, b) \in f$.

99. **Definition.** Suppose that $f : A \to B$. The set A is called the **domain** of f. The set B is called the **codomain** or **target space** of f. The **range** of f is the set of all $b \in B$ such that there exists $a \in A$ with $f(a) = b$.

100. **Remark.** In the text a definition of equality of two functions is given. The definition in the text is not a standard definition. Here is my definition.

101. **Definition.** We say that two functions $f : A \to B$ and $g : C \to D$ are equal if and only if $A = C$, $B = D$, and the set f is equal to the set g.

102. **Remark.** Two functions f and g from A to B are equal if and only if for every $a \in A$, $f(a) = g(a)$.

103. **Definition and Remark.** Suppose that $f : A \to B$. We say that f is **injective** or **one-to-one** if and only if for all $a_1 \in A$ and $a_2 \in A$ if $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$. We say that f is **surjective** or **onto** if and only if for every $b \in B$ there exists $a \in A$ with $f(a) = b$. We say that f is **bijective** if and only if f is injective and surjective.

    Note that f is injective if and only if for all $a_1 \in A$ and $a_2 \in A$ if $f(a_1) = f(a_2)$ then $a_1 = a_2$. Note also that f is surjective if and only if B is the range of f.

104. **Remark.** Suppose that $f : A \to B$. Then f is bijective if and only if for every $b \in B$ there is a unique $a \in A$ such that $f(a) = b$.

105. **Remark (Pigeon Principle, function version).** Suppose that A and B are finite sets and $f : A \to B$.

    If $|A| > |B|$, then f is not injective.

    If $|A| < |B|$, then f is not surjective.

    If $|A| = |B|$, then f is injective if and only if f is surjective.

106. **Definition.** Suppose that $f : A \to B$ and $g : B \to C$. Then the **composition** is the function $g \circ f : A \to C$ defined as follows: If $a \in A$ then $(g \circ f)(a) = g(f(a))$.

107. **Theorem.** Suppose that $f : A \to B$ and $g : B \to C$. If f and g are injective, then $g \circ f$ is injective. If f and g are surjective, then $g \circ f$ is surjective.

108. **Theorem.** Composition of functions is associative. That is, if $f : A \to B$, $g : B \to C$ and $h : C \to D$ are functions, then

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

109. **Definition.** Suppose that f is a relation from A to B. The **inverse relation** of f is the relation from B to A given by

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

110. **Remark and Theorem.** Suppose that $f : A \to B$. Then f is also a relation from A to B. So the inverse relation f^{-1} is defined and is a relation from B to A. We have the following theorem: f^{-1} is a function from B to A if and only if f is bijective.

111. **Definition.** Let A be a set. The **identity function** on A is the function $i_A : A \to A$ given by $i_A(x) = x$ for every $x \in A$.

112. **Theorem.** Suppose that $f : A \to B$ is bijective. Then $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

113. **Theorem:** Suppose that $f : A \to B$ and $g : B \to A$. Suppose also that $g \circ f = i_A$ and $f \circ g = i_B$. Then f and g are bijective and $g = f^{-1}$.

114. **Theorem:** Suppose that $f : A \to B$ and $g : B \to A$. Suppose the following holds:

$$\forall x \in A, \forall y \in B, (f(x) = y \Leftrightarrow g(y) = x).$$

Then $g \circ f = i_A$ and $f \circ g = i_B$. So, f and g are bijective and $g = f^{-1}$.

115. **Theorem:** Suppose that $f : A \to B$ and $g : B \to C$. Suppose that f and g are bijective. Then $g \circ f$ is bijective and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

116. **Definition.** Suppose that $f : A \to B$.

If $X \subseteq A$, the **image** of X is the set $f(X) = \{f(x) : x \in X\}$.

If $Y \subseteq B$, the **preimage** of Y is the set

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

Notes for Chapter 14

117. **Definition.** We say that two sets A and B have the **same cardinality**, written $|A| = |B|$, if and only if there is a bijective function $f : A \to B$.

118. **Proposition**. Suppose that A, B, C are sets. Then:

1. $|A| = |A|$.
2. If $|A| = |B|$, then $|B| = |A|$.
3. If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

119. **Theorem:** Suppose that A is a set. Then there does not exist a surjective function $f : A \to \mathscr{P}(A)$. So A and $\mathscr{P}(A)$ do not have the same cardinality.

120. **Theorem (Cantor-Bernstein-Schroder Theorem):** Suppose that A and B are sets. Suppose that there exist injective functions $f : A \to B$ and $g : B \to A$. Then A and B have the same cardinality.