BCM I : Final 2012

June 20, 2012

ID#: Name:

1. Let P, Q, R be statements. (10 pts)

   (a) Complete the following truth table. (6 pts)

P	Q	R	$P \Rightarrow (Q \wedge R)$	$(P \wedge \sim Q) \vee (P \wedge \sim R)$
T	T	T		
T	T	F		
T	F	T		
T	F	F		
F	T	T		
F	T	F		
F	F	T		
F	F	F		

   (b) Let $X = P \Rightarrow (Q \wedge R)$ and $Y = (P \wedge \sim Q) \vee (P \wedge \sim R)$. Determine true of false of each of the following. (4 pts)

   (i) $X \equiv Y$ (True, False) (ii) $X \equiv \sim Y$ (True, False)

   (iii) $X \vee Y$ is tautology (True, False) (iv) $X \vee \sim Y$ is tautology (True, False)

2. Prove the following. (10 pts)

   (a) The square of an odd integer is congruent to 1 modulo 8.

   (b) The sum of the squares of two odd integers cannot be a perfect square.

1.	2.	3*.	4*.	5*.	6.	7.	Total

ID#: Name:

3. Let n be a (fixed) positive integer. For $a, b \in \boldsymbol{Z}$, we write $a \equiv b \pmod{n}$, whenever there is an integer c such that $b - a = cn$.

   (a) Show that $a \equiv b \pmod{n}$ is an equivalence relation of $\boldsymbol{Z}$. (10 pts)

   (b) For $a \in \boldsymbol{Z}$, $[a] = \{x \in \boldsymbol{Z} \mid x \equiv a \pmod{n}\}$. Show that $a \equiv b \pmod{n}$ if and only if $[a] = [b]$. (5 pts)

   (c) Show that $\{[0], [1], \ldots, [n-1]\}$ is a partition of $\boldsymbol{Z}$. (5 pts)

ID#: Name:

4. Let $f : X \to Y$, $g : Y \to Z$ and $h = g \circ f : X \to Z$ $(x \mapsto g(f(x)))$ be functions.

   (a) Show that if both f and g are onto, then so is h. (5 pts)

   (b) Show that if h is one-to-one, then so is f. (5 pts)

   (c) First show that if A and B are subsets of X, then $f(A \cap B) \subseteq f(A) \cap f(B)$. Next give an example that $f(A \cap B) \neq f(A) \cap f(B)$. (5 pts)

   (d) Show that if A is a subset of X and C a subset of Y, then $f(A \cap f^{-1}(C)) = f(A) \cap C$. (5 pts)

ID#: Name:

5. Let $(-\pi/2, \pi/2) = \{x \in \boldsymbol{R} : -\pi/2 < x < \pi/2\}$, and $[-\pi/2, \pi/2] = \{x \in \boldsymbol{R} : -\pi/2 \leq x \leq \pi/2\}$.

   (a) State the definition of $|A| = |B|$ for sets A, B, and show that $|(-\pi/2, \pi/2)| = |\boldsymbol{R}|$. (Hint: $\tan(x)$) (10 pts)

   (b) Show $|[-\pi/2, \pi/2]| = |\boldsymbol{R}|$. (10 pts)

6. Let $f : X \to Y$ is an onto function. State the definition of $|A| \leq |B|$ for sets A, B and show that for any set Z, $|\mathrm{Map}(Y, Z)| \leq |\mathrm{Map}(X, Z)|$. (10 pts)

ID#: Name:

7. For nonzero integers a and b, the greatest common divisor $d = \gcd(a, b)$ is a positive integer satisfying the following. (i) $d \mid a$ and $d \mid b$. (ii) If $c \mid a$ and $c \mid b$, then $c \mid d$. In the following we will show that there exist $s, t \in \boldsymbol{Z}$ such that $d = as + bt$, where $d = \gcd(a, b)$. Let $S = \{ax + by > 0 \mid x, y \in \boldsymbol{Z}\}$. (10 pts)

   (a) Show that $S \neq \emptyset$.

   (b) Let $d = \min S$. Show that $d \mid a$ and $d \mid b$.

   (c) Show that $d = \min S$ is the greatest common divisor.

Please write your comments:

(1) About this course, especially suggestions for improvements.

(2) Topics in Mathematics or in other subjects you want to pursuit.

BCM I: Solutions to Final 2012

June 20, 2012

1. Let P, Q, R be statements. (10 pts)

   (a) Complete the following truth table. (6 pts)

   Soln.

P	Q	R	$P \Rightarrow (Q \wedge R)$	$(P \wedge \sim Q) \vee (P \wedge \sim R)$
T	T	T	$T \quad \boldsymbol{T} \quad T$	$F \quad \boldsymbol{F} \quad F$
T	T	F	$T \quad \boldsymbol{F} \quad F$	$F \quad \boldsymbol{T} \quad T$
T	F	T	$T \quad \boldsymbol{F} \quad F$	$T \quad \boldsymbol{T} \quad F$
T	F	F	$T \quad \boldsymbol{F} \quad F$	$T \quad \boldsymbol{T} \quad T$
F	T	T	$F \quad \boldsymbol{T} \quad T$	$F \quad \boldsymbol{F} \quad F$
F	T	F	$F \quad \boldsymbol{T} \quad F$	$F \quad \boldsymbol{F} \quad F$
F	F	T	$F \quad \boldsymbol{T} \quad F$	$F \quad \boldsymbol{F} \quad F$
F	F	F	$F \quad \boldsymbol{T} \quad F$	$F \quad \boldsymbol{F} \quad F$

   (b) Let $X = P \Rightarrow (Q \wedge R)$ and $Y = (P \wedge \sim Q) \vee (P \wedge \sim R)$. Determine true of false of each of the following. (4 pts)

   (i) $X \equiv Y$ (True, $\boxed{\text{False}}$) (ii) $X \equiv \sim Y$ ($\boxed{\text{True}}$, False)

   (iii) $X \vee Y$ is tautology ($\boxed{\text{True}}$, False) (iv) $X \vee \sim Y$ is tautology (True, $\boxed{\text{False}}$)

2. Prove the following. (*These are taken from homework.*) (10 pts)

   (a) The square of an odd integer is congruent to 1 modulo 8.

   Soln. Let a be an odd integer. Then there exists an integer n such that $a = 4n \pm 1$. Now

$$a^2 = (4n \pm 1)^2 = 16n^2 \pm 8n + 1 = 8(2n^2 \pm n) + 1.$$

   (b) The sum of the squares of two odd integers cannot be a perfect square.

   Soln. By (a), if a and b are odd integers, there exist an integer m such that

$$a^2 + b^2 = 8m + 2 = 4(2m) + 2.$$

   Suppose $a^2 + b^2 = c^2$ for some integer c. Then c^2 is even. Hence c is even. Let $c = 2s$. Then $c^2 = 4s^2$ and it is divisible by 4. This is a contradiction as $a^2 + b^2 = 4(2m) + 2$ is not divisible by 4.

3. Let n be a (fixed) positive integer. For $a, b \in \boldsymbol{Z}$, we write $a \equiv b \pmod{n}$, whenever there is an integer c such that $b - a = cn$.

   (a) Show that $a \equiv b \pmod{n}$ is an equivalence relation of $\boldsymbol{Z}$. (10 pts)

   Soln. (i) Since $a - a = 0 = 0n$, $a \equiv a \pmod{n}$. (Reflexive)

   (ii) Suppose $a \equiv b \pmod{n}$. Then there is an integer c such that $b - a = cn$. Thus $a - b = (-c)n$ and $b \equiv a \pmod{n}$. (Symmetric)

   (ii) Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then there are integers c and d such that $b - a = cn$ and $c - b = dn$. Thus $c - a = (c - b) + (b - a) = cn + dn = (c + d)n$ and $a \equiv c \pmod{n}$. (Transitive)

   Since the relation satisfies reflexive, symmetric and transitive properties, it is an equivalence relation.

(b) For $a \in \boldsymbol{Z}$, $[a] = \{x \in \boldsymbol{Z} \mid x \equiv a \pmod{n}\}$. Show that $a \equiv b \pmod{n}$ if and only if $[a] = [b]$. (5 pts)

Soln. Suppose $a \equiv b \pmod{n}$. Let $x \in [a]$. Then $x \equiv a \pmod{n}$. By transitivity, $x \equiv b \pmod{n}$, and $x \in [b]$. Thus $a \equiv b \pmod{n}$ implies $[a] \subseteq [b]$.

By symmetricity, $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$. Hence by replacing a with b, we have $[b] \subseteq [a]$. Therefore $[a] = [b]$.

Conversely suppose $[a] = [b]$. Then by reflexivity, $a \equiv a \pmod{n}$ and $a \in [a]$. Therefore $a \in [b]$ and $a \equiv b \pmod{n}$.

(c) Show that $\{[0], [1], \ldots, [n-1]\}$ is a partition of $\boldsymbol{Z}$. (5 pts)

Soln. For $m \in \boldsymbol{Z}$, there exist unique integers q, r such that $m = qn + r$ with $0 \leq r \leq n-1$. Since $m - r = qn$, $m \equiv r \pmod{n}$ and $[m] = [r]$ for unique element in $\{[0], [1], \ldots, [n-1]\}$. Since $m \in [m] = [r]$,

$$\boldsymbol{Z} = [0] \cup [1] \cup \cdots \cup [n-1], \text{ and } [i] \cap [j] = \emptyset \text{ if } 0 \leq i < j \leq n-1.$$

Since $i \in [i]$, each of $[0], [1], \ldots, [n-1]$ is nonempty. Therefore $\{[0], [1], \ldots, [n-1]\}$ is a partition of $\boldsymbol{Z}$.

4. Let $f : X \to Y$, $g : Y \to Z$ and $h = g \circ f : X \to Z$ $(x \mapsto g(f(x)))$ be functions.

(a) Show that if both f and g are onto, then so is h. (5 pts)

Soln. Let $z \in Z$. Since $g : Y \to Z$ is onto, there is $y \in Y$ such that $g(y) = z$. Now since $f : X \to Y$ is onto and $y \in Y$, there is $x \in X$ such that $f(x) = y$. Therefore, $x \in X$ safisties

$$h(x) = g(f(x)) = g(y) = z.$$

Thus $h : X \to Z$ is onto.

(b) Show that if h is one-to-one, then so is f. (5 pts)

Soln. For $x_1, x_2 \in X$, suppose $f(x_1) = f(x_2)$. We will show that $x_1 = x_2$. By definition,

$$h(x_1) = g(f(x_1)) = g(f(x_2)) = h(x_2).$$

Since h is one-to-one, $x_1 = x_2$, and f is one-to-one as desired.

(c) First show that if A and B are subsets of X, then $f(A \cap B) \subseteq f(A) \cap f(B)$. Next give an example that $f(A \cap B) \neq f(A) \cap f(B)$. (5 pts)

Soln. Let $x \in A \cap B$. Since $x \in A$, $f(x) \in f(A)$. Similarly, since $x \in B$, $f(x) \in f(B)$. Thus $f(x) \in f(A) \cap f(B)$. Therefore $f(A \cap B) \subseteq f(A) \cap f(B)$.
Let $X = \{1, 2\}$, $Y = \{0\}$, $A = \{1\}$. $B = \{2\}$ and $f(1) = f(2) = 0$. Then

$$f(A \cap B) = f(\emptyset) = \emptyset \neq \{0\} = f(\{1\}) \cap f(\{2\}) = f(A) \cap f(B).$$

This is an example that $f(A \cap B) \neq f(A) \cap f(B)$.

(d) Show that if A is a subset of X and C a subset of Y, then $f(A \cap f^{-1}(C)) = f(A) \cap C$. (5 pts)

Soln. Since $f^{-1}(C) = \{x \in X \mid f(x) \in C\}$, $f(f^{-1}(C)) \subseteq C$, by (c),

$$f(A \cap f^{-1}(C)) \subseteq f(A) \cap f(f^{-1}(C)) \subseteq f(A) \cap C.$$

Let $c \in f(A) \cap C$. Since $c \in f(A)$, there is $a \in A$ such that $f(a) = c$. Since $f(a) = c \in C$, $a \in f^{-1}(C)$. Therefore $a \in A \cap f^{-1}(C)$, $c = f(a) \in f(A \cap f^{-1}(C))$ and $f(A) \cap C \subseteq f(A \cap f^{-1}(C))$.

5. Let $(-\pi/2, \pi/2) = \{x \in \boldsymbol{R} : -\pi/2 < x < \pi/2\}$, and $[-\pi/2, \pi/2] = \{x \in \boldsymbol{R} : -\pi/2 \le x \le \pi/2\}$.

   (a) State the definition of $|A| = |B|$ for sets A, B, and show that $|(-\pi/2, \pi/2)| = |\boldsymbol{R}|$. (Hint: $\tan(x)$) (10 pts)

   Soln. For sets A, B, $|A| = |B|$ if and only if $A = B = \emptyset$ or there is a bijection, $f : A \to B$. Let $f : (-\pi/2, \pi/2) \to \boldsymbol{R}$ $(x \mapsto \tan(x))$. Since $f'(x) = \sec^2(x) = 1/\cos^2(x) > 0$, $f(x)$ is strictly increasing in the interval and it is one-to-one as $f(x_1) < f(x_2)$ whenever $-\pi/2 < x_1 < x_2 < \pi/2$. Moreover, $f(x)$ is continuous and

$$\lim_{x \to \pi/2-} f(x) = \lim_{x \to \pi/2-} \tan(x) = \infty, \text{ and } \lim_{x \to -\pi/2+} f(x) = \lim_{x \to -\pi/2+} \tan(x) = -\infty.$$

   Hence by the intermediate value theorem, f is onto. Therefore f is a bijection and $|(-\pi/2, \pi/2)| = |\boldsymbol{R}|$.

   (b) Show $|[-\pi/2, \pi/2]| = |\boldsymbol{R}|$. (10 pts)

   Soln. Let $g : [-\pi/2, \pi/2] \to \boldsymbol{R}$ $(x \mapsto x)$ and $h : \boldsymbol{R} \to [-\pi/2, \pi/2]$ $(x \mapsto f^{-1}(x))$, where $f(x) = \tan(x)$ as in (a) (in particular $f^{-1}(x) = \arctan(x)$). Since f is a bijection, h is one-to-one. Since g is clearly one-to-one, by the Schröder-Bernstein Theore, there is a bijection from $[-\pi/2, \pi/2]$ to $\boldsymbol{R}$ and $|[-\pi/2, \pi/2]| = |\boldsymbol{R}|$.

6. Let $f : X \to Y$ is an onto function. State the definition of $|A| \le |B|$ for sets A, B and show that for any set Z, $|\mathrm{Map}(Y, Z)| \le |\mathrm{Map}(X, Z)|$. (10 pts)

   Soln. For sets A, B, $|A| \le |B|$ whenever $A = \emptyset$ or there is a one-to-one function from A to B.

   If $Z = \emptyset$, $\mathrm{Map}(Y, Z) = \emptyset$ and there is nothing to prove. Now let

$$F : \mathrm{Map}(Y, Z) \to \mathrm{Map}(X, Z)\ (g \mapsto g \circ f).$$

   Since $f : X \to Y$ and $g : Y \to Z$, $g \circ f \in \mathrm{Map}(X, Z)$. We will show that F is one-to-one. Suppose $F(g_1) = F(g_2)$ for $g_1, g_2 \in \mathrm{Map}(Y, Z)$. Since $F(g_1), F(g_2) \in \mathrm{Map}(X, Z)$, $F(g_1) = F(g_2)$ implies that for all $x \in X$,

$$g_1(f(x)) = (g_1 \circ f)(x) = F(g_1)(x) = F(g_2)(x) = (g_2 \circ f)(x) = g_2(f(x)).$$

   Now for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$ by assumption. Hence $g_1(y) = g_2(y)$ for every $y \in Y$ by above. Thus $g_1 = g_2$ and F is one-to-one.

7. For nonzero integers a and b, the greatest common divisor $d = \gcd(a, b)$ is a positive integer satisfying the following. (i) $d \mid a$ and $d \mid b$. (ii) If $c \mid a$ and $c \mid b$, then $c \mid d$. In the following we will show that there exist $s, t \in \boldsymbol{Z}$ such that $d = as + bt$, where $d = \gcd(a, b)$. Let $S = \{ax + by > 0 \mid x, y \in \boldsymbol{Z}\}$. (10 pts)

   (a) Show that $S \neq \emptyset$.

   Soln. Since a and b are nonzero, $0 < a^2 + b^2 \in S$ by taking $x = a$ and $y = b$. Thus $S \neq \emptyset$.

   (b) Let $d = \min S$. Show that $d \mid a$ and $d \mid b$.

   Soln. Since $d \in S$, there exist $s, t \in \boldsymbol{Z}$ such that $d = as + bt$. Let $a = dq + r$ where $q, r \in \boldsymbol{Z}$ and $0 \le r < d$. Then $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq)$. Since $r < d = \min S$, $r \notin S$. Thus $r = 0$ and $d \mid a$. Similarly we have $d \mid b$.

   (c) Show that $d = \min S$ is the greatest common divisor.

   Soln. Since $d \in S$, $d > 0$. Hence by (b) we only need to show (ii). Suppose $c \mid a$ and $c \mid b$. So there are $a', b' \in \boldsymbol{Z}$ such that $a = ca'$ and $b = cb'$. Since $d = as + bt = ca's + cb't = c(a's + b't)$, $c \mid d$ as desired.

数学通論 I を受講したみなさんへ

Grading Policy

最初に配布したシラバスにあるように、演習 (Recitation) (30%) （12 回分割り当てました)、宿題 (Homework) (20%) （8 回、80 問提出を求めました)、期末試験 (Final) (50%) （6 月 20 日に実施)。

教員によって考え方はことなりますが、私は、授業科目というより、コースという考え方が、学士課程教育では大切だと思っています。このコースで 10 週間かけてどれだけ学んだかが重要です。学んだ内容も、学び全体の中でそれをどのように位置づけるかも、ひとそれぞれでしょう。そこで、今までの課題を丁寧に提出し、演習の問題の大部分を黒板で発表してきた人は単位を落とすことはありません。ただし、この評価の仕方では、期末試験の割合を高くしてあります。数学において、学んだ数学を試験で表現できることは大切だと考えているからです。

Final および提出物は週明けには返却できると思います。返却できるようになった時点で Moodle に書き授業支援室 H113 で受け取るようにします。H113 閉室のときは H109 で受け取って下さい。

専門の数学の最初のコースはどうでしたか。楽しめましたか。お疲れ様。

After BCM I

まずは、夏の数学セミナーへ参加して下さると嬉しいですね。(8/27-8/30 ICU 軽井沢キャンパスの予定)。今年の教科書は田村一郎 「解析入門」です。また、教科書の第 12 章を読むことを勧めます。微分積分学を復習することにもなりますし、数学通論 II への橋渡しにもなります。数学通論に関連して、ちょっと堅めに夏やすみのお薦めを書きます。

1. 数学通論 III の参考書となっている「集合と位相」内田伏一著、裳華房 の前半が集合論です。
2. 数学通論 II に関係する、高木貞治「解析概論」を最初からじっくり読むのがお薦め。
3. 線型代数特論（旧・線形代数学 III）を履修する人も多いと思います。佐武一郎著「線型代数入門」を最初からじっくり読むのもお薦め。
4. もう少し簡単に取り組めそうなのは、「集合への 30 講」志賀浩二著　朝倉書店。
5. 公理的集合論入門をかじってみたい人には、「新装版：集合とはなにか (はじめて学ぶ人のために)」竹内外史著、講談社。

私は、一年生の夏休みは岩村聯著「束論」を読み通しました。これが数学の本で初めて読み通したものでした。

二年生の夏は記憶が定かではありませんが松坂和夫著「集合と位相」を読んだと思います。全部は読まなかったかも知れません。個人的には、上の 1 にかわるものとしておすすめです。しかし恐らく絶版。

三年生の夏には「集合論入門」赤摂也著、培風館（ISBN4-563-00301-8, 1957.1.25）を短期間に読み通しました。集合と位相関係の本が並びましたが、無論、他にも読みました。Serge Lang の Algebra は一年生の秋から、3 人で自主ゼミをして読み、4 年まで続けました。完全には終わりませんでした。ポントリャーギンの「連続群論」上下も 3 人での自主ゼミをながいことしましたが、上巻しかゼミでは終わりませんでした。ポントリャーギンの「常微分方程式」はかなり進みましたが、読み終わったかどうかはあまりよく覚えていません。コルモゴロフ・フォミーンの「関数解析の基礎」は読み始めましたが、問題が難しく、あまり進みませんでした。

夏休みにじっくり一冊、数学の本を読むことに時間をかけることができれば、たとえ、読む量は少なくても、大きな価値があると思いますよ。数学で学んだことは何年かたって、誤りだったということも、時代遅れになることもありません。また、苦労して読む経験はすべて脳のトレーニングになっているハズです。数学を楽しみましょう。

鈴木寛 (*hsuzuki@icu.ac.jp*)