

Archive for
MATH 123, Abstract Mathematics 1, Fall 2024

Bilkent University, Laurence Barker, 27 January 2024.

Source file: arch123fall24.tex

page 2: Course specification.

page 5: Quizzes.

page 11: Homework.

page 23: Midterm 1.

page 24: Solutions to Midterm 1.

page 28: Midterm 1 Retake.

page 29: Solutions to Midterm 1 Retake.

page 30: Midterm 2.

page 31: Solutions to Midterm 2.

page 34: Final.

page 35: Solutions to Final.

Course specification

MATH 123, *Abstract Mathematics 1*, Fall 2024

Laurence Barker, Bilkent University. Version: 5 December 2024.

Course Aims: One of the two main aims is to acquire the ability to produce mathematical proofs. That includes: an ability to fully understand definitions and hypotheses, an ability to argue deductively from hypotheses to conclusions, an ability to communicate mathematics using unambiguous statements, an ability to assess whether a given argument is valid.

The other main aim is to acquire knowledge and understanding of certain fundamental concepts, most notably: statements, sets, functions, the field of real numbers, countability.

Course Description: This course lays the groundwork for all pure mathematics and all theoretically advanced applied mathematics. It will proceed slowly, because different students are likely to have very different mathematical backgrounds. For the entertainment of those students who already have substantial relevant experience, there will be some hard exercises. But the priority will be on getting everyone or almost everyone ready for the rest of the mathematics program.

Course Requirements: Curiosity about mathematics. Intellectual integrity.

Instructor: Laurence Barker, Office SA 129, barker at fen dot bilkent dot edu dot tr.

Assistant: Mahmut Esat Akin.

Texts:

Required textbook:

- Steven Galovich, “Introduction to Mathematical Structures”, (Harcourt Brace Jovanovich, 1989.)

Recommended texts:

- Daniel W. Cunningham, “Logical Introduction to Proof”, Springer, 2012.
- Joseph Fields, “A Gentle Introduction to the Art of Mathematics”, version 3.1, self-published, 2013.
- Daniel Rosenthal, David Rosenthal, Peter Rosenthal, “A Readable Introduction to Real Mathematics”, Springer, 2014.
- Ted Sunderstrom, “Mathematical Reasoning Writing and Proof”, version 2.1, self-published, 2022.
- Daniel J. Vellerman, “How To Prove It”, 2nd edition, Cambridge University Press, 1994.

See also supplementary material on my homepage

<http://www.fen.bilkent.edu.tr/~barker/fenis2.html>

and on Moodle.

Classes: Mondays 15:30 - 17:20, Thursdays 10:30 - 12:20, room B-Z01.

Office Hours: Tuesdays, 12:30 - 13:10, in my office, room SA-129.

Office hours is for *all* the students on the course, the flying, the swimming and the drowning. Although you are welcome to come after a disaster, that will not unstich the past. It is much better to come *before* the prospective disaster.

Weekly Syllabus

The format below is, *Week number; Monday date; Subtopics*.

- 1:** 16 Sept: Intuitive notions of the natural numbers, rational integers, rational numbers, real numbers, complex numbers, quaternions. The question of the existence of a square root of -1 . Pythagoras' Theorem and the question of the existence of a square root of 2.
- 2:** 23 Sept: Statements. Truth tables. Universal and existential quantifiers. Sets as collections.
- 3:** 30 Sept: Functions as operations. Universal and existential quantifiers. Illustrations including limits, continuity, uniform continuity.
- 4:** 7 Oct: Russell's Paradox. Set theoretic constructions, including pairs. Functions as correspondences. Injections, surjections, bijections.
- 5:** 14 Oct: Equivalence relations. The natural numbers as the cardinalities of the finite sets. Principle of mathematical induction. Binomial coefficients and the Binomial Theorem.
- 6:** 21 Oct: Rings and ring isomorphisms. Construction of the integers.
- 7:** 28 Oct, *with holiday on Monday and Tuesday*: Fields. Construction of the field of rational numbers.
- 8:** 4 Nov: The Euclidian algorithm. Prime numbers. Fundamental Theorem of Arithmetic.
- 9:** 11 Nov: Ideals. Congruence classes of integers. Fermat's Little Theorem. Chinese Remainder Theorem.
- 10:** 18 Nov: Cantor's construction of the real number field as a quotient of the ring of Cauchy sequences.
- 11:** 25 Nov: Complex numbers, quaternions, 2×2 rings of matrices. Some ring isomorphisms.
- 12:** 2 Dec: Countability. Cantor's diagonal argument. The Schröder-Bernstein Theorem. The uncountability of the reals.
- 13:** 9 Dec: Further exercises on countability and cardinality.
- 14:** 16 Dec: [*Further selected topic, if time permits.*]
- 15:** 23 Dec, *only Monday and Tuesday*: Review.

Assessment:

A minimum of 75% attendance is required.

- Quizzes 10%.
- Midterm 1, 25%. 17:30 - 19:30, Wednesday 6 November, SA Z18, SA Z19, SA Z20.
- Midterm 1 Retake, 25%, 17:30 - 19:30, Wednesday 4 December, B Z08.
- Midterm 2, 25%. 17:30 - 19:30, Monday 9 December, SA Z01, SB Z03.
- Final, 40%.

Midterm 1 Retake conditions: Those who scored less than 50% in Midterm 1 and who did a script postmortem with me during week 10 are eligible for the retake. Their recorded score will be $\max(50, \min(m_1, r_1))$ where m_1 is the Midterm 1 score and r_1 is the Midterm 1 Retake score.

FZ criteria: Severe failure to demonstrate comprehension of core concepts. Severe failure to communicate mathematical reasoning using grammatical sentences.

Speaking: All speaking in class must address everyone in the room. Questions and comments are welcome: they make learning easier, and they make teaching easier too.

Class Announcements: All students, including any absentees from a class, will be deemed responsible for awareness of class announcements.

Quizzes, with solutions

Laurence Barker, 13 December 2024

Quiz 1: Let $I = \{2, 3, 5, 7, 9\}$ and $J = \{12, 9, 5\}$. Evaluate:

(a) $I \cup J$,

(a) $I \cap J$.

Solution: Obviously, $I \cup J = \{2, 3, 5, 7, 9, 12\}$ and $I \cap J = \{5, 9\}$.

Quiz 2: Let $g : Z \leftarrow Y$ and $f : Y \leftarrow X$ be functions such that $g \circ f$ is surjective.

(a) Must g always be surjective?

(b) Must f always be surjective?

Justify you answers by proof or counter-example.

Solution: Part (a): Yes. Given any $z \in Z$, we are to show that there exists $y \in Y$ such that $z = g(y)$. By the surjectivity of $g \circ f$, there exists $x \in X$ such that $z = g(f(x))$. So we can put $y = f(x)$.

Part (b). No. One counter-example is the case where the sets are $Z = Y = \{1, 2\}$ and $X = \{1\}$, the functions are $g = \text{id}_X = \text{id}_Y$ and f is either one of the two functions $Y \leftarrow X$.

Practice Quiz, not credited: Consider the real sequences x with mutually distinct terms and with length 100. What is the largest value of n such that:

(a) There is an increasing subsequence of length n for all such x ?

(b) There is an decreasing subsequence of length n for all such x ?

(c) There is an increasing or decreasing subsequence of length n for all such x ?

Part (a). The answer is $n = 1$, which occurs when x is decreasing.

Part (b). The answer is $n = 1$, which occurs when x is increasing.

Part(c). The answer is $n = 10$. Indeed, the Erdős–Szekeres Theorem tells us that every real sequence with mutually distinct terms and length at least $9^2 + 1 = 82$ has an increasing or decreasing sequence with length $9+1 = 10$. On the other hand, since $100 = 10 \cdot 10$, the corollary we proved shows that there exists some x with no increasing or decreasing subsequence longer than 10.

Comment: This kind of question, requiring great care over *exactly* what is being said, arises very frequently in mathematics. The trick of guessing what is meant just by picking up the vocabulary and using the context (which I do a lot when listening to Turkish) is absolutely not going to work here. Often in mathematics, it is necessary to get the quantification $\forall$ and $\exists$ exactly right.

Quiz 3: (a) State any version of the Erdős–Szekeres Theorem.

(b) Let n be a positive integer. Does every infinite sequence of real numbers has a monotonic subsequence with length n ?

Solution 3: Part (a). Given a sequence x of mutually distinct real numbers such that x has length greater than n^2 , then x has a monotonic subsequence of length greater than n .

Part (b). Yes. Let x be an infinite sequence of real numbers. If x has infinitely many terms equal to some real number c , then the infinite subsequence consisting of those terms is monotonic. Otherwise, we can replace x with the infinite subsequence y obtained from x by deleting all terms that repeat previous terms. By the theorem, the first $n^2 + 1$ terms of y have a monotonic subsequence with length $n + 1$.

Alternative Solution 3: Part (a). Given a sequence x of real numbers such that x has length greater than n^2 , then x has a monotonic subsequence of length greater than n .

Part (b). Yes. Let x be an infinite sequence of real numbers. By the theorem, the first $n^2 + 1$ terms of x have a monotonic subsequence with length $n + 1$.

Comment 1: This course is not aimed at solving standard problems using standard routines. We are to reason deductively about general theory. To do that, we must know the standard theorems and standard definitions. And we must also be able to express statements clearly. So we must be able to state the theorems and the definitions.

So it is appropriate for quiz and exam questions to demand statements of theorems and definitions. Trying to memorize them without understanding them is the road to a dark place. The trick is to *understand* them and also to learn how to express statements clearly. Then, from your understanding of a theorem or definition, you will be able to compose a suitable statement.

Comment 2: The Erdős–Szekeres Theorem was not originally intended to be on the syllabus. I introduced it as a reaction to the difficulty some of us were having with the abstract material. It is just a nice example of a theorem whose proof can be easily understood without any abstract concepts.

But I find that there are two versions of the theorem in the literature, one of them including the condition that the terms are mutually distinct. That condition makes things a little more straightforward, but it is not really needed.

Comment 3: For some other questions along these lines, see Homework 2.

Quiz 4: We define the **negative** $-\alpha$ of an element $\alpha \in \mathbb{Z}/n$ to be such that, if $\alpha = [x]_n$ with $x \in \mathbb{Z}$, then $-\alpha = [-x]_n$. Show that $-\alpha$ is well-defined.

Solution 4: Let $x, x' \in \mathbb{Z}$ such that $\alpha = [x]_n = [x']_n$. Then $x \equiv_n x'$, so $-x \equiv_n -x'$, hence $[-x]_n = [-x']_n$.

Comment: Arguably, the required conclusion is simply obvious. At any rate, this is an easy question and almost any correct observations along the above lines are likely to be enough to ensure that the required conclusion is entirely clear.

In the solution above, for even more detail, we could have appended the line: “Thus, we have shown that the defining equality for $-\alpha$ is independent of the choice of x .” But that extra line is not really a necessity.

Quiz 5: Use the Euclidean algorithm to find $\gcd(1024, 150)$. No use of prime factorization is permitted.

Solution 5: We have $\gcd(1024, 150) = 2$ because

$$1024 = 6 \cdot 150 + 124, \quad 150 = 1 \cdot 124 + 26, \quad 124 = 4 \cdot 26 + 20, \quad 26 = 1 \cdot 20 + 6, \quad 20 = 3 \cdot 6 + 2, \quad 6 = 3 \cdot 2 + 0.$$

Comment: Of course, the question would be easier if we were permitted to use the prime factorizations $1024 = 2^{10}$ and $150 = 2 \cdot 3 \cdot 5^2$. But, when the prime factors of a and b are large and unknown, $\gcd(a, b)$ tends to be easier to calculate using the Euclidian algorithm rather than the prime factorizations.

Quiz 6: Show that $1^3 + 2^3 + \dots + n^3 = n^2(n+1)^2/4$ for all positive integers n .

Solution 6: Let S_n and T_n , respectively, be the left hand side and the right hand side of the required equation. We shall show, by induction, that $S_n = T_n$. The case $n = 1$ is trivial. Now suppose that $n \geq 2$ and that $S_{n-1} = T_{n-1}$. A straightforward calculation shows that $T_n - T_{n-1} = S_n - S_{n-1}$. Hence, $S_n = T_n$.

Alternative Solution 6: For a contradiction, let n be minimal such that $S_n \neq T_n$, where S_n and T_n , respectively, are the expressions on the left and on the right of the required equation. We have $S_1 = T_1$, so $n \geq 2$. But $T_n - T_{n-1} = S_n - S_{n-1}$ by an easy calculation. Hence $S_{n-1} \neq T_{n-1}$, which contradicts the minimality of n .

Another Alternative Solution 6: The expression S_n on the left is characterized by the initial condition $S_1 = 1$ and the recurrence relation $S_n - S_{n-1} = n^3$ for $n \geq 2$. The expression T_n on the right plainly satisfies $T_n = 1$. A direct calculation shows that $T_n - T_{n-1} = n^3$ for $n \geq 2$.

Comment 1: In the short term, you might manage okay by just copying the above phrasing without actually understanding the argument. But that is a nicely paved road to failure. To learn to do mathematics, you must follow the reasoning, not the phrasing.

Comment 2: The third argument shows that explicit appeal to mathematical induction is not necessary. Sure enough, that argument does make an implicit appeal to fundamental properties of the natural numbers, say, the Peano Axioms, including the Principle of Mathematical Induction, but it does not require the reader to have been explicitly introduced to any of those axioms.

Quiz 7: Let $x_0, x_1, \dots$ be the infinite sequence such that $x_{n+2} = 5x_{n+1} - 6x_n$ for all $n \in \mathbb{N}$, also $x_0 = 2$ and $x_1 = 5$. Show that $x_n = 2^n + 3^n$ for all n .

Solution 7: Let $y_n = 2^n + 3^n$. We have $y_0 = 2$ and $y_1 = 5$. Now suppose, inductively, that $x_n = y_n$ and $x_{n+1} = y_{n+1}$. Noting that $t = 2$ and $t = 3$ are solutions to $t^2 - 5t + 6 = 0$, we see that

$$y_{n+2} - 5y_{n+1} + 6y_n = 0 = x_{n+2} - 5x_{n+1} + 6x_n.$$

Since $-5y_{n+1} + 6y_n = -5x_{n+1} + 6x_n$, we deduce that $y_{n+2} = x_{n+2}$.

Alternative solution: The alternative solution to the previous quiz question can be adapted in a straightforward way.

Comment: Again, follow the reasoning, not the phrasing

Quiz 8: Find the greatest common divisor of $(X - 1)^2$ and $X^2 - 1$ in the ring $\mathbb{R}[X]$.

Solution 8: We have $X^2 - 1 = (X - 1)(X + 1)$, so $X - 1$ divides both of the given polynomials. If $f(X)(X - 1)$ divides both of the given polynomials, then plainly $f(X) = c$ for some nonzero real number c . So the greatest common divisor is $X - 1$.

Comment 1: In $\mathbb{R}[X]$, the greatest common divisor of two nonzero elements is well-defined up to a factor in $\mathbb{R}$. That is to say, the greatest common divisors of $(X - 1)^2$ and $X^2 - 1$ are the polynomials $c(X - 1)$ where c is a nonzero real number. In general, for suitable rings where greatest common divisors can be defined (called principal ideal domains), they well-definedness is up to multiplication by a unit. For the ring $\mathbb{Z}$, the only units are 1 and -1 . Given nonzero integers a and b , we conventionally take the greatest common divisor g of a and b to be positive, but $-g$ has the same essential feature, to wit, an integer c divides a and b if and only if c divides $-g$.

Comment 2: This question was set as a way of indicating that the theory we did for $\mathbb{Z}$ can be adapted for some other rings, including $\mathbb{R}[X]$. A good exercise is to work through the whole proof of the Fundamental Theorem of Arithmetic, starting from the examination of the Euclidian Algorithm. By the time you have finished, you will thoroughly understand that tract of classical number theory.

Quiz 9: Find integers u and v such that $\gcd(126, 303) = 126u + 303v$.

Solution 9: We have

$$303 = 2 \cdot 126 + 51, \quad 126 = 2 \cdot 51 + 24, \quad 51 = 2 \cdot 24 + 3, \quad 24 = 8 \cdot 3 + 0.$$

So $\gcd(126, 303) = 3$. We have

$$3 = 51 - 2 \cdot 24 = 51 - 2(126 - 2 \cdot 51) = 5 \cdot 51 - 2 \cdot 126 = 5(303 - 2 \cdot 126) - 2 \cdot 126 = 5 \cdot 303 - 12 \cdot 126.$$

So we can put $u = -12$ and $v = 5$.

For a ring R , we define a **unit** of R to be an element $u \in R$ such that there exists $v \in R$ satisfying $uv = 1_R = vu$. By an argument similar to the proofs of the uniqueness of 0_R and 1_R , it is easy to show that, if u is a unit, then there exists a unique $v \in R$ such that $uv = 1_R = vu$. We call v the **inverse** of u and write $v = u^{-1}$.

Quiz 10: Let R be a ring. We define a relation $\equiv$ on R such that, given $a, b \in R$, then $a \equiv b$ if and only if there exists a unit $u \in R$ such that $a = ubu^{-1}$. Show that $\equiv$ is an equivalence relation.

Solution 10: Let $a, b, c \in R$. Noting that 1_R is a unit with inverse $(1_R)^{-1} = 1_R$, we have $a = 1_R a (1_R)^{-1}$. Thus, $\equiv$ is reflexive. Suppose $a \equiv b$. Let u be a unit such that $a = ubu^{-1}$. Noting that u^{-1} is a unit and with inverse u , we have $b = u^{-1} a (u^{-1})^{-1}$, in other words, $b \equiv a$. Thus, $\equiv$ is symmetric. Finally, suppose $a \equiv b$ and $b \equiv c$. Let u and v be units such that $a = ubv$ and $b = vcv^{-1}$. Noting that $uvv^{-1}u^{-1} = 1_R = v^{-1}u^{-1}uv$, we see that uv is a unit with $(uv)^{-1} = v^{-1}u^{-1}$. So $a = uvcv^{-1}u^{-1} = uvc(uv)^{-1}$. Thus, $\equiv$ is transitive.

Comment: I set this as a variant of Question 1 in Retake Midterm 1. I think maybe we have now very clearly reached the fork in the road.

Some students eventually catch onto mathematics and can produce the above kind of argument. Other students never learn how to do it and, quite simply, remain unable to do conceptual mathematics. So let us discuss this in detail.

The Eternal Fundamental Human Conversation:

Soft culture person: Please give me the fish.

Hard culture person: I do not have any fish.

Soft: You promised you would return with some fish for me.

Hard: No. What I said was that if you give me the fishing net, then I will return with some fish for you. But you did not give me the net.

Soft: Please do not get logical with me. You know I failed Abstract Survival 123. The only bit I understood was that you would give me some fish. So kindly now give me the fish.

Hard: Let me try to explain it this way. Take P to be the statement: you give me the net. Take Q to be the statement: I give you some fish. What I said was that P implies Q . Alas, Q is false. But P is also false. So what I said is true.

Soft: Yes, you mentioned the net already. But let us stick to the bit I understand, which is about you giving me the fish. Kindly give me the fish.

Hard: But that was conditional upon your giving me the net.

Soft: Yes, but let us not talk about the net. I just want the fish.

Hard: But, but, but...

Version based on discussions concerning Q1 in Retake and Quiz 10:

Student: $a = uau^{-1}$ so $a \equiv a$.

Teacher: What is u here?

Student: It is the u that you mentioned in the question.

Teacher: But the existence of that that u was conditional upon having $a \equiv b$. We are now considering the case where a is any element of R and $b = a$. We want to show that the condition $a \equiv a$ holds. In other words, we want to find a u such that $a = uau^{-1}$. Is there such a u ?

Student: I interpreted the question in a different way, with u decided from the beginning.

Teacher: But, but, but...

I keep trying to understand what is going on here. There are two main ways of thinking about mathematics, roughly:

Platonism: Mathematical objects exist and they are somehow related to rocks and electricity, which is why mathematicians, together with some assistants, are able to produce aeroplanes and telephones.

Formalism: The logic of fantasy mathematical objects is related to the logic of rocks and electricity, which is why mathematicians and some assistants are able to produce aeroplanes and telephones.

Since my thinking is of the former kind, and since I have never been in the position of the above students, I am guessing that the students must be thinking in the latter way. I am guessing that the students are imitating previous equivalence relation arguments, adapting them to the notation at hand. Some of the nonsensical solutions to Retake Question 1 had clauses quoted from the equivalence relation in the construction of the rational numbers.

Imitation might work in some disciplines. It does not work in advanced mathematics. In rare cases, genius level imitation combined with an ability to do calculation routines can lead to passes in some courses. However, such students are always guessing. They can never be sure of any mathematical statement unless they have learned it from someone they trust. They

cannot do a project that requires independent study. To produce a project, they either have to copy it or else every step has to be given to them by a teacher.

Not being able to do the quiz question is okay. To do it completely, you had to notice, for instance, that $(uv)^{-1} = v^{-1}u^{-1}$. But, if you could not do it, then you should at least have recognized that there were some technical problems that you could not solve: after arriving at $a = uvcv^{-1}u^{-1}$, your trouble was that you could not see why there is a unit w such that $a = wcw^{-1}$.

If you were writing things like, “if $a = ubu^{-1}$ and $b = ucu^{-1}$ then $a = ucu^{-1}$ ”, then I suggest you read the above solution again, but now thinking of R as a thing with properties, elements of R as things with properties, statements as expressions of those properties. Do not think of statements as phrases of formal birdsong that have to fit with some ritual patterns.

I want to believe that you can all do conceptual mathematics, and that something just needs to click so that you start thinking in the right kind of way. You may have to unlearn the calculation procedure mathematics that is taught at school.

Quiz 11: Let R be a ring. We define a relation $\sim$ on R such that, given $a, b \in R$, then $a \sim b$ if and only if there exists a unit $u \in R$ such that $a = ub$. Show that $\sim$ is an equivalence relation.

Solution 11: Let $a, b, c \in R$. We have $a = 1_R a$, so $a \sim a$. If $a \sim b$, say $a = ub$ with u a unit, then $b = u^{-1}a$, hence $b \sim a$. Suppose $a \sim b$ and $b \sim c$. Then $a = ub$ and $b = vc$ where u and v are units. We have $a = uvc$, hence $a \sim c$. Thus, we have proved that $\sim$ is reflexive, symmetric, transitive.

Quiz 12: Let $(a_0, a_1, \dots)$ be a Cauchy sequence of rational numbers. Suppose x converges to 0, that is to say, given rational $\epsilon > 0$ then, for sufficiently large n , we have $|a_n| < \epsilon$. Let $b \in \mathbb{Q}$. Show that the sequence $xb = (a_0b, a_1b, \dots)$ converges to 0. (Hint: deal separately with the case where $b = 0$.)

Solution 12: The case where $b = 0$ is trivial, so we may assume that $b \neq 0$. For all sufficiently large n , we have $|a_n| < \epsilon/|b|$, hence $|a_nb| < \epsilon$.

Homework

MATH 123, *Abstract Mathematics 1*, Fall 2024, Laurence Barker

version: 19 December 2024

Homework 1: Set on 23 September.

The solutions are to be discussed in the following week, Monday 30th to Thursday 4th October.

At this stage in the course, we have not established enough material for systematic exercises. So we can play.

Exercise 1.A is very easy. The first quiz will be something similar.

For all the other exercises, you are *expected* to get into trouble in some way or another! It does not matter, since there is no course credit for it. The main purpose is to collide with some difficulties which you might not be ready for. That might then motivate the prerequisite theory.

Exercise 1.1: Let $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$. Evaluate:

(a) $A \cup B$.

(c) $A \cap B$.

Exercise 1.2: Let a be a rational integer. Show that there do not exist rational integers b and c such that $4a + 3 = b^2 + c^2$.

Exercise 1.3: Let a, b, c be real numbers with $a \neq 0$. Define $\Delta = b^2 - 4ac$. Prove that:

(a) If $\Delta > 0$, then there are exactly 2 real numbers x satisfying $ax^2 + bx + c = 0$, namely $(-b + \sqrt{\Delta})/2a$ and $(-b - \sqrt{\Delta})/2a$.

(b) If $\Delta = 0$, then there is exactly 1 real number x such that $ax^2 + bx + c = 0$, namely $-b/2a$.

(c) If $\Delta < 0$, then there are no real numbers x satisfying $ax^2 + bx + c = 0$.

Exercise 1.4: Let n be a positive integer and let $x_1, \dots, x_n, y_1, \dots, y_n$ be real numbers. Show that

$$\left(\sum_i x_i y_i \right)^2 \leq \left(\sum_j x_j^2 \right) \left(\sum_k y_k^2 \right).$$

Hint: use Exercise 1.3.

Exercise 1.5: With the notation in the previous exercise, show that

$$\sqrt{\sum_i (x_i - y_i)^2} \leq \sqrt{\sum_j x_j^2} + \sqrt{\sum_k y_k^2}.$$

Exercise 1.6: Let n be a positive integer and let $a_1, \dots, a_n$ be positive real numbers such that $\sum_i a_i = 1$. Show that the smallest possible value of $\sum_i 1/a_i$ is n^2 . Hint: Use Exercise 1.A.

The next two questions are more open ended, because we have not yet established the fundamental properties of the complex numbers and the quaternions. So, if you get stuck wondering exactly what features may be assumed, then that may reinforce the point that precise definitions and proofs of fundamental properties are important.

Exercise 1.7: Recall, $i^2 = -1$ and the complex numbers are such that every complex number z can be expressed in only one way as $z = x + iy$. Assume that the complex numbers behave according to some familiar laws of arithmetic, such as $z_1 + z_2 = z_2 + z_1$. Show that there are exactly two complex numbers z satisfying $z^2 + 1 = 0$.

Exercise 1.8: Recall,

$$i^2 = j^2 = k^2 = ijk = -1$$

and the quaternions are such that every quaternion w can be expressed in only one way as $w = t + ix + jy + kz$ where x, y, z are real numbers. Assume that the quaternions behave according to some familiar laws of arithmetic, except that w_1w_2 is not always equal to w_2w_1 . Show that there are infinitely many quaternions w satisfying $w^2 + 1 = 0$.

Homework Solutions 1

1.1: Plainly, $A \cup B = \{1, 2, 3, 4, 5, 6\}$ and $A \cap B = \{3, 4\}$.

Comment: A proof explains an assertion by breaking up its content into steps, each step being obvious. If one tries to break up each obvious step into smaller obvious steps, then the argument will become harder to understand. If one keeps breaking up obvious steps into smaller obvious steps, then one will never finish.

So, if an assertion is obvious, then proof unnecessary and it would be impossible to produce anyway. However, it is sometimes helpful to inform the reader that an assertion is obvious. The words “obviously”, “plainly”, “clearly” are useful for warning a reader not to overthink an obvious assertion.

1.2: Given $a, b, c \in \mathbb{Z}$ then, upon division by 4, the remainders of $4a + 3$ and b^2 and c^2 are 3 and β and γ where $\beta, \gamma \in \{0, 1\}$. So $4a + 3 \neq b^2 + c^2$.

1.3: First suppose $\Delta \geq 0$. Let $\delta = \sqrt{\Delta}$. Let $\alpha = (-b + \delta)/2a$ and $\beta = (-b - \delta)/2a$. Then, $\alpha + \beta = -b/a$ and $\alpha\beta = (b^2 - \delta^2)/4a^2 = c/a$. So, for all $x \in \mathbb{R}$, we have

$$(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta = x^2 + (b/a)x + (c/a).$$

Since $a \neq 0$, the real number

$$ax^2 + bx + c = a(x - \alpha)(x - \beta)$$

is 0 if and only if $x = \alpha$ or $x = \beta$. Note that $\Delta = 0$ if and only if $\alpha = \beta$, in which case, $\alpha = -b/2a$. We have established parts (a) and (b).

Now suppose $ax^2 + bx + c = 0$ for some real number x . Then

$$0 = x^2 + (b/a)x + c/a = (x - b/2a)^2 - b^2/4a^2 + c/a = (x - b/2a)^2 - \Delta/4a^2.$$

Hence $\Delta \geq 0$. We have established part (c).

Flawed solution: Suppose $ax^2 + bx + c = 0$. Then

$$0 = x^2 + (b/a)x + c/a = (x - b/2a)^2 - b^2/4a^2 + c/a = (x - b/2a)^2 - \Delta/4a^2.$$

Hence $\Delta \geq 0$. So (c) holds.

Let $\delta = \sqrt{\Delta}$. Let $\alpha = (-b + \delta)/2a$ and $\beta = (-b - \delta)/2a$. We have $x - b/2a = \pm\delta/2a$. So $x = \alpha$ and $x = \beta$.

Comment: The flawed solution is incomplete because it failed to check that, when $\Delta \geq 0$, both α and β are solutions. All it showed is:

If a solution x exists, then $x = \alpha$ or $x = \beta$.

It failed to confirm that, when $\Delta \geq 0$, a solution exists. Let us give an example of how that kind of reasoning can lead to a false conclusion.

Exercise: Find all the real numbers x such that $x^2 = -1$.

Flawed solution: Suppose $x^2 = -1$. Then $x^4 = 1$. Therefore, $x = 1$ or $x = -1$. In conclusion, the real numbers x satisfying $x^2 = -1$ are 1 and -1 .

Homework 2

The references are to the Galovich textbook.

Sets: page 135 Questions 2.3.6, 2.3.8, 2.3.14; page 137 Questions 3, 5, 7, 10.

Equivalence relations: page 180, Questions 3.3.1, 3.3.8, 3.3.10, 3.3.20.

Cardinality: page 217, Questions 4.1.1, 4.1.4, 4.1.7.

Some questions on the Erdős–Szekeres Theorem.

Recall, a finite or infinite sequence of real numbers $x = (x_1, x_2, \dots)$ is said to be:

- **increasing** provided $x_i \leq x_j$ whenever $i \leq j$,
- **decreasing** provided $x_i \geq x_j$ whenever $i \leq j$,
- **strictly increasing** provided $x_i < x_j$ whenever $i < j$,
- **strictly decreasing** provided $x_i > x_j$ whenever $i > j$,
- **constant** provided $x_i = x_j$ for all indices i and j .

2.1 Let p, q, r be positive integers. State and prove an analogue of the Erdős–Szekeres Theorem that has the conclusion “Then x has a strictly increasing subsequence with length p or a constant subsequence with length q or a strictly decreasing subsequence with length r ”.

2.2: Show that, for every positive integer n , every infinite real sequence x has a monotonic subsequence with length n .

2.3: Does every infinite real sequence have an infinite subsequence that is strictly increasing or constant or strictly decreasing?

Homework Solutions 2

Galovich 3.3.8, part (a): Let $\sim$ be the relation on $\mathbb{N} \times \mathbb{N}$ such that $(a, \alpha) \sim (b, \beta)$ if and only if $a + \beta = b + \alpha$. Show that $\sim$ is an equivalence relation.

Solution: Let $x = (a, \alpha)$ and $y = (b, \beta)$ and $z = (c, \gamma)$ be elements of $\mathbb{N} \times \mathbb{N}$. The relation $\sim$ is reflexive, indeed, it is obvious that $x \sim x$. Also $\sim$ is symmetric, indeed, it is obvious that if $x \sim y$ then $y \sim x$. For transitivity, suppose $x \sim y$ and $y \sim z$. Thus, $a + \beta = b + \alpha$ and $b + \gamma = c + \beta$. Hence

$$a + \beta + \gamma = b + \alpha + \gamma = c + \alpha + \beta.$$

We deduce that $a + \gamma = c + \alpha$, in other words, $x \sim z$.

Comment: An alternative would be to note that $x \sim y$ if and only if $a - \alpha = b - \beta$. It follows that $\sim$ is the equivalence relation associated with the function $\mathbb{Z} \leftarrow \mathbb{N} \times \mathbb{N}$ given by $a - \alpha \mapsto (a, \alpha)$.

But this question is used to construct $\mathbb{Z}$ as the set of equivalence classes of $\sim$. For that purpose, of course, the alternative argument cannot be used, indeed, we may not make use of $\mathbb{Z}$ until we have constructed it.

Hint 2.1: Let p, q, r be positive integers and let x be a real sequence of length greater than pqr . Then x has a strictly increasing subsequence with length p or a constant subsequence with length q or a strictly decreasing subsequence with length r .

Concise proof: Write $x = (x_0, \dots, x_{pqr})$. For each $0 \leq i \leq pqr$, let a_i, b_i, c_i , respectively, be the lengths of the longest strictly increasing, constant, strictly decreasing subsequences starting at the term x_i in position i . The argument proceeds much as in the proof of the named theorem, but now with the triples (a_i, b_i, c_i) , which are shown to be mutually distinct.

2.3: Yes. Let $x = (x_1, x_2, \dots)$ be an infinite real sequence. Let I be the set of indices i such that $x_i \leq x_j$ for all $j \geq i$. If I is infinite, the x has an infinite increasing subsequence. Suppose I is finite. Let k be a natural number greater than every element of I . Removing the first k terms from x , we reduce to the case where $I = \emptyset$. Then x has an infinite decreasing subsequence.

Relations, homework exercises

1.1: Let n be a positive integer and X a set with size n . How many:

- (1) relations on X are there?
- (2) reflexive relations on X are there?
- (3) symmetric relations on X are there?
- (4) antisymmetric relations on X are there?
- (5) reflexive symmetric relations on X are there?

We did most of the following exercise in class, but with a different notation and, in particular, different roles for lower case Roman, upper case Roman, lower case Greek letters. Use notes from that if you wish, but if you just copy without thinking, you will get it wrong. Understanding requires an ability to recognize an argument when it appears with a different notation.

1.2: Define $\mathbb{Z}' = \mathbb{Z} - \{0\}$ and define $\approx$ be the relation on $\mathbb{Z} \times \mathbb{Z}'$ such that, given $\mu, \nu \in \mathbb{Z} \times \mathbb{Z}'$, writing $\mu = (u, U)$ and $\nu = (v, V)$, then $\mu \approx \nu$ provided $uV = vU$. Show that $\approx$ is an equivalence relation.

If you can, do this question without using division. That way, starting from $\mathbb{Z}$, we can define $\mathbb{Q}$ to be the set of equivalence classes under $\approx$. Thus,

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}') / \approx .$$

To put it another way,

$$\mathbb{Q} = \{[\mu]_{\approx} : \mu \in \mathbb{Z} \times \mathbb{Z}'\} .$$

Again, writing $[u, U] = [(u, U)]_{\approx}$, we have

$$\mathbb{Q} = \{[u, U] : (u, U) \in \mathbb{Z} \times \mathbb{Z}'\} .$$

We can regard $\mathbb{Z}$ as a subset of $\mathbb{Q}$ by identifying each $u \in \mathbb{Q}$ with $[u, 1]$.

1.3: Let $\equiv$ be the relation on $\mathbb{Q}$ such that, given $x, y \in \mathbb{Q}$, then $x \equiv y$ if and only if $x - y$ is an integer. Show that $\equiv$ is an equivalence relation.

1.4: Let n be a natural number and X a set with size n . Let $\subseteq_X$ be the usual subset relation on the power set $\mathcal{P}(X)$. For which values of n is $\subseteq_X$:

- (1) an equivalence relation?
- (2) a total ordering?
- (3) a partial ordering?

1.5: Let m and n be positive integers and let $x_0, \dots, x_n$ be a sequence of mutually distinct real numbers. Let $N = \{0, \dots, mn\}$. Write $\sqsubseteq$ for the relation on N such that $i \sqsubseteq j$ provided $i \leq j$ and $x_i \leq x_j$. Show that $\sqsubseteq$ is a partial ordering.

Comment: That easy exercise will be used in the hard exercises at the end of this document.

Well-definedness, homework exercises

2.1: Let $f : Y \leftarrow X$ be a function. Define a relation $\equiv_f$ on X such that, given $x, x' \in X$, then $x \equiv_f x'$ if and only if $f(x) = f(x')$. Obviously, $\equiv_f$ is an equivalence relation. Write $[x]_f = [x]_{\equiv_f}$. Is there a well-defined function $Y \leftarrow X/\equiv_f$ given by $f(x) \mapsto [x]_f$?

2.2: In the notation of Exercise 1.2, consider the set $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}')/\approx$. We define the **sum** of elements μ and ν of $\mathbb{Q}$ to be the element

$$\mu + \nu = [uV + vU, UV]$$

where (u, U) and (v, V) are choices of elements of $\mathbb{Z} \times \mathbb{Z}$ satisfying $\mu = [u, U]$ and $\nu = [v, V]$. We define the **product** of μ and ν to be the element

$$\mu\nu = [uv, UV] .$$

Show that the sum and product are well-defined.

2.3: Let $\equiv$ be the relation on $\mathbb{Q}$ defined in Exercise 1.3.

(1) Is there a well-defined sum on $\mathbb{Q}/\equiv$ given by the formula $[x] + [y] = [x + y]$?

(2) Is there a well-defined product on $\mathbb{Q}/\equiv$ given by the formula $[x][y] = [xy]$?

Mathematical induction, homework exercises

Each exercise in this section can be done using any one of the following techniques:

- direct recursive argument,
- mathematical induction,
- well-ordering principle and argument by contradiction.

In each case, the choice is yours, but I suggest you frame your arguments using mathematical induction, just to practice that technique.

The **Fibonacci sequence** is defined to be the infinite sequence $F_0, F_1, \dots$ such that

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

for all natural numbers n . We call F_n the **Fibonacci number** indexed by n .

The Fibonacci numbers were discussed by Virahanka, in the 6th, 7th or 8th century, in the context of counting the number of ways of speaking continuously for n units of time using a 1 unit syllable and a 2 unit syllable. See Exercise 3.1. Hints at this application to the study of poetic metre appeared in earlier Indian work, some of it in the 1st millenium BC.

3.0: By experimenting with small values of n , guess a formula for $1 - 2^2 + 3^2 - \dots + (-1)^{n-1}n^2$, then prove it.

3.1: Let n be a natural number. Show that F_{n+1} is the number of tuples $(x_1, \dots, x_m)$ such that $x_1 + \dots + x_m = n$ and each $x_i \in \{1, 2\}$.

3.2: Prove that $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ for all positive integers n .

Comment: The equality in that question is called **Cassini's identity**. It was noted by Giovanni Domenico Cassini in 1680.

3.3: Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. Show that $F_n = \frac{\phi^n - \psi^n}{\sqrt{5}} = \frac{\phi^n - \psi^n}{\phi - \psi} = \sum_{i=0}^n \phi^i \psi^{n-i}$.

Comment: The real number ϕ is called the **Golden ratio**.

3.4: Recall

$$\binom{n}{r} = \begin{cases} n!/r!(n-r)! & \text{if } 0 \leq r \leq n, \\ 0 & \text{otherwise} \end{cases}$$

for any positive integer n and any integer r . Also recall, Pascal's Identity is

$$\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}$$

for all integers n with $n \geq 2$ and all integers r . Using Pascal's Identity, prove the Binomial Theorem.

Classical number theory, homework exercises

4.1: Let $g = \gcd(5852, 4641)$.

(1) Evaluate g .

(2) Find Bézout coefficients for 5852 and 4641. In other words, find integers x and y such that $g = 5852x + 4641y$.

4.2: By analogy with the theory for $\mathbb{Z}$, state and prove versions of the Euclidian algorithm, greatest common divisor, Fundamental Theorem of Arithmetic for polynomial rings over fields.

Solution 4.1: For part (1), we have

$$5852 = 1 \cdot 4641 + 1211, \quad 4641 = 3 \cdot 1211 + 1008, \quad 1211 = 1 \cdot 1008 + 203,$$

$$1008 = 4 \cdot 203 + 196, \quad 203 = 1 \cdot 196 + 7, \quad 196 = 28 \cdot 7.$$

So $g = 7$. For part (2), we have

$$\begin{aligned} 7 &= 203 - 196 = 203 - (1008 - 4 \cdot 203) = 5 \cdot 203 - 1008 = 5(1211 - 1008) - 1008 \\ &= 5 \cdot 1211 - 6 \cdot 1008 = 5 \cdot 1211 - 6(4641 - 3 \cdot 1211) = 23 \cdot 1211 - 6 \cdot 4641 \\ &= 23 \cdot 1211 - 6(5852 - 1211) = 29 \cdot 1211 - 6 \cdot 5852. \end{aligned}$$

So we can put $x = -6$ and $y = 5$.

Hard homework exercises

Material relating to the next three exercises can be found in the Wikipedia entries for Mirsky's Theorem, Dilworth's Theorem, the Erdős–Szekeres Theorem. The notation there is different. If you use that material, make sure you fully understand it and convert to the notation below.

H.1 Given a poset P , then any subset $S \subseteq P$ becomes a poset with the restricted partial ordering relation. When S is a toset, we call S a **chain** in P . When $x \not\leq y$ for all distinct x and y in S , we call S an **antichain**.

(1) Suppose P is finite. For each $x \in P$, let $H(x)$ be the maximum size of a chain with maximum element x . Show that, for any positive integer i , the preimage $H^{-1}(i)$ is an antichain.

(2) Using part (1), prove the following theorem.

Mirsky's Theorem: *Given a finite poset P , then the maximum size of a chain in P is the minimum number k such that P is the union of k antichains.*

Comment Mirsky's Theorem was given by Leon Mirsky in 1971.

H.2: Prove the following theorem. An outline for a proof, using induction on the size of the poset, is given below.

Dilworth's Theorem: *Given a finite poset P , then the maximum size of an antichain in P is the minimum number w such that P is the union of w chains.*

(1) Show that, if P is the disjoint union of w chains $D_1, \dots, D_w$ and P has an antichain B with size w , then $D_i \cap B \neq \emptyset$ for each i .

(2) Let a be a maximal element of P and let $Q = P - \{a\}$ as a subposet. Let v be the maximum size of an antichain of Q . Assume, inductively, that the required conclusion holds for Q . Let $C_1, \dots, C_v$ be mutually disjoint chains whose union is Q . Let $A = \{a_1, \dots, a_v\}$ where each a_i is the maximal element of C_i such that a_i belongs to an antichain of size v . Show that A is an antichain.

(3) In the case where $a_i \leq a$ for some i , complete the proof of the theorem by considering the subposet obtained from P by removing a and those $x \in C_i$ such that $x \leq a_i$.

(4) In the case where $a_i \not\leq a$ for all i , complete the proof by observing that the singleton set $\{a\}$ is both a chain and an antichain.

Comment: Dilworth's Theorem was given by Robert Dilworth in 1950. The proof outlined above is due to Fredrick William Galvin, 1994. The number w is called the **width** of P .

H.3: Previously, we proved the following theorem using the Pigeonhole Principle.

Erdős–Szekeres Theorem: *Let m and n be positive integers. Let x be a finite real sequence with length greater than mn . Then x has an increasing subsequence with length greater than m or a decreasing subsequence with length greater than n .*

(1) Give a proof of the Erdős–Szekeres Theorem using Mirsky's Theorem.

(2) Give proof of the Erdős–Szekeres Theorem using Dilworth's Theorem.

Hint: For both parts, use the partial ordering $\sqsubseteq$ that appeared in Exercise 1.5. For $\sqsubseteq$, what are the chains and what are the antichains?

Comment: The proof of the Erdős–Szekeres Theorem by applying theory of posets to $\sqsubseteq$ is due to John Michael Steel, 1995.

Solutions to the hard exercises

H.1: Part (1). For a contradiction, suppose $H^{-1}(i)$ is not an antichain. Then $x < y$ for some $x, y \in H^{-1}(i)$. A chain with size i with maximum element x can be extended to a chain with length $i + 1$ with maximum element y . We deduce that $H(y) > i$, contradicting the condition $y \in H^{-1}(i)$.

Part (2). Let j be the maximum size of a chain in P . Then

$$P = \bigcup_{s=1}^j H^{-1}(s) .$$

By part (1), $k \leq j$. For the converse, let C be a chain with length j . Let $A_1, \dots, A_k$ be antichains whose union is P . Then

$$P = \bigcup_{i=1}^k (C \cap A_i) .$$

But $|C \cap A_i| = 1$ for all i . So $k \leq j$. We conclude that $j = k$.

H.2: Part (1). Given $x, y \in D_i \cap B$ then $x \leq y$ or $y \leq x$ because $x, y \in D_i$. On the other hand, $x \not\leq y$ and $y \not\leq x$ because $x, y \in B$. Therefore, $x = y$. We have shown that $|D_i \cap B| \leq 1$. But

$$B = \bigcup_{i=1}^w (D_i \cap B) .$$

Since $|B| = 1$, each $|D_i \cap B| = 1$.

Part (2). For each i , let A_i be an antichain of size v such that $a_i \in A_i$. Suppose $a_i \leq a_j$. We must show that $a_i = a_j$. Let $x \in C_i \cap A_j$. Since x is an element of C_i belonging to an antichain of size v , the definition of a_i implies that $x \leq a_i$. By transitivity, $x \leq a_j$. But x and a_j both belong to the antichain A_j , so $x = a_j$. Therefore, $a_j \leq a_i$. By antisymmetry, $a_i = a_j$.

Part (3). As we saw in part (1), the intersection of a chain and an antichain always has size at most 1. So it suffices to show that there exists some u such that P has an antichain with size u and P is the union of u chains.

Let R be the specified subposet of P . Then R is a subposet of Q , so R is the union of v chains. We claim that R is the union of $v - 1$ chains. We may assume that $C_i \cap R \neq \emptyset$, since otherwise the claim is clear. By the definition of a_i , the chain $C_i \cap R$ does not intersect with an antichain of Q with size v . Therefore, $C_i \cap R$ does not intersect with an antichain of R with size v . By part (1), R does not have an antichain with size v . But $A - \{a_i\}$ is an antichain of R with size $v - 1$. We have shown that $v - 1$ is the maximum size of an antichain in R . By an inductive argument, the claim follows. We have $P = R \cup (P - R)$, moreover, $P - R$ is a chain, so P is the union of v chains.

Meanwhile A is an antichain in P with size v . So we can put $u = v$ and we have completed the proof of the theorem in this case.

Part (4). By the first paragraph of part (3), it suffices to show that P has an antichain with size $v + 1$ and P is the union of $v + 1$ chains. Since a is maximal in P , the set $A \cup \{a\}$ is an antichain with size $v + 1$. Since $\{a\}$ is a chain, P is the union of the chains $\{a\}, C_1, \dots, C_v$.

H.3: We may assume that x has length $mn + 1$ and we can write $x = (x_0, \dots, x_{mn})$. Let $P = \{0, \dots, mn\}$ as a poset with the specified partial ordering $\sqsubseteq$. Let $I = \{i_0, \dots, i_k\}$ be a

subset of $\{0, \dots, mn\}$ with $i_0 < \dots < i_k$. Let $x_I = (x_{i_0}, \dots, x_{i_k})$. Then I is a chain in P if and only if x_I is an increasing subsequence. Also, I is an antichain in P if and only if I is a strictly decreasing subsequence.

Part (1). Suppose x has no increasing subsequence of length greater than m , in other words, P has no chain of length greater than m . By Mirsky's Theorem, P is the union of m antichains. Since $|P| > mn$, the average size of those antichains is greater than n . Therefore, one of those antichains has size greater than n . That is to say, P has a strictly decreasing subsequence of length greater than n .

Part (2). The argument is similar to that of part (1), with the roles of chains and antichains interchanged.

MATH 123: Abstract Mathematics 1

Midterm 1



6 November 2024, Laurence Barker

The duration of the exam is 120 minutes.

Please write your name clearly on every sheet of your script.

If you do not write in complete sentences, the examiner will still try to understand what you are saying. But you are strongly advised to write in complete sentences, because that will probably help the examiner understand what you are saying.

No notes or texts may be used during the exam, nor electronic devices, nor red pens, nor very faint pencils.

Do take the question sheet home. No writing on handed in question sheets will be marked.

1: (20 marks.) Let $\sim$ be the relation on $\mathbb{N} \times \mathbb{N}$ such that, given $x, y \in \mathbb{N} \times \mathbb{N}$, writing $x = (a, \alpha)$ and $y = (b, \beta)$, then $x \sim y$ provided $a - b + 2(\alpha - \beta) = 0$. Is $\sim$ an equivalence relation? (Most of the marks are for the justification, not the answer.)

2: (30 marks.) Let n be an integer with $n \geq 4$. Let X be a set with size $|X| = n$. Let $Y_1 = \{1\}$ and $Y_2 = \{1, 2\}$ and $Y_3 = \{1, 2, 3\}$. Let $k \in \{1, 2, 3\}$. Your answers to the following should be in terms of k . For parts (a), (b), (c), just the easy answer will do and no explanation is required. Most of the marks are for parts (d) and (e).

(a) For $k \in \{1, 2, 3\}$, how many injections $Y_k \rightarrow X$ are there?

(b) For $k \in \{1, 2, 3\}$, how many injections $X \rightarrow Y_k$ are there?

(c) For $k \in \{1, 2, 3\}$, how many functions $X \rightarrow Y_k$ are there?

(d) For $k \in \{1, 2, 3\}$, how many surjections $X \rightarrow Y_k$ are there? (Justify your answer.)

(e) Consider the equivalence relations $\equiv$ on X such that $\equiv$ has at most 3 equivalence classes. How many such equivalence relations $\equiv$ are there? (Justify your answer.)

3: (30 marks) (a) Show that, given non-empty sets A and B , then there exists an injection $A \rightarrow B$ if and only if there exists a surjection $B \rightarrow A$. (This is a standard result, but you must give a proof.)

(b) State the Schröder–Bernstein Theorem. (Just state any standard version, no proof needed.)

(c) Let A, B, C be non-empty sets such that there exist injections $A \rightarrow B$ and $B \rightarrow C$ and $C \rightarrow A$. Without using any theory of cardinal numbers, just using standard results about injections, surjections and bijections, show that there exist bijections $A \rightarrow B$ and $B \rightarrow C$ and $C \rightarrow A$.

4: (20 marks.) You may assume the following fact, which comes from number theory: There is an infinite subset Π of $\mathbb{N}$ such that, for any mutually distinct elements $p_1, \dots, p_r$ of Π and any natural numbers $a_1, \dots, a_r, b_1, \dots, b_r$ satisfying

$$p_1^{a_1} p_2^{a_2} \dots p_{r-1}^{a_{r-1}} p_r^{a_r} = p_1^{b_1} p_2^{b_2} \dots p_{r-1}^{b_{r-1}} p_r^{b_r}$$

we have $a_i = b_i$ for all $i \in \{1, \dots, r\}$.

Let $\mathcal{P}$ denote the set whose elements are the finite subsets of $\mathbb{N}$. Show that $|\mathcal{P}| = |\mathbb{N}|$. (Any correct argument will do. You may use the above fact from number theory if you wish.)

Solutions to Midterm 1

1: Let $x, y, z \in X$. Write $x = (a, \alpha)$ and $y = (b, \beta)$ and $z = (c, \gamma)$. Obviously, $x \sim x$, in other words, $\sim$ is reflexive. Obviously, if $x \sim y$ then $y \sim x$, in other words, $\sim$ is symmetric. Suppose $x \sim y$ and $y \sim z$. Then $a + 2\alpha = b + 2\beta = c + 2\gamma$, so $x \sim z$. We have confirmed that $\sim$ is transitive.

2: Part (a). The answer is $\begin{cases} n & \text{if } k = 1, \\ n(n-1) & \text{if } k = 2, \\ n(n-1)(n-2) & \text{if } k = 3. \end{cases}$

Part (b). The answer is 0.

Part (c). The answer is k^n .

Part (d). Let s_k denote the number of surjections $X \rightarrow Y_k$. Obviously, $s_1 = 1$. Every function $X \rightarrow Y_2$ is surjective except for the 2 functions whose image is singleton. So, using part (c), $s_2 = 2^n - 2$. Since s_3 depends only on n , we may assume that $X = \{1, 2, 3\}$. For $i \in X$, let A_i be the set of functions $X \rightarrow Y_3$ whose image does not own i . By part (c), $|A_i| = 2^n$ and $|A_i \cap A_j| = 1$ whenever $i \neq j$. Also, $|A_1 \cap A_2 \cap A_3| = 0$. Therefore,

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| - |A_1 \cap A_3| - |A_1 \cap A_2| = 3(2^n - 1).$$

By part (c) again, $s_3 = 3^n - |A_1 \cup A_2 \cup A_3| = 3^n - 3 \cdot 2^n + 3$. In conclusion,

$$s_k = \begin{cases} 1 & \text{if } k = 1, \\ 2^n - 2 & \text{if } k = 2, \\ 3^n - 3 \cdot 2^n + 3 & \text{if } k = 3. \end{cases}$$

Part (e). Any surjection $f : X \rightarrow Y_k$ gives rise to an equivalence relation $\equiv_f$ on X such that the equivalence classes under $\equiv_f$ are the preimages of the elements of Y_k . Each equivalence relation on X with exactly k equivalence classes arises in this way from exactly $k!$ surjections f . So the number of equivalence relations on X with exactly k equivalence classes is $s_k/k!$. Therefore, the number of the specified kind of equivalence relation is

$$s_1 + \frac{s_2}{2!} + \frac{s_3}{3!} = 1 + \frac{2^n - 2}{2} + \frac{3^n - 3 \cdot 2^n + 3}{6} = \frac{3^{n-1} + 1}{2}.$$

3: Part (a). First suppose there is an injection $f : A \rightarrow B$. Choose $a_0 \in A$. We define a function $g : B \rightarrow A$ as follows. Given $b \in \text{im}(f)$, we define $g(b) = a$ where a is the unique element of A such that $f(a) = b$. Given $b \in B - \text{im}(f)$, we define $g(b) = a_0$. Plainly, g is surjective.

Conversely, suppose there is a surjection $g : B \rightarrow A$. We define a function $f : A \rightarrow B$ such that, given $a \in A$, then $f(a) = b$ where b is a chosen element of B satisfying $a = g(b)$. Plainly, f is injective.

Part (b). Given sets A and B such that there exists an injection $A \rightarrow B$ and an injection $B \rightarrow A$, then there exists a bijection $A \rightarrow B$.

Part (c). The composite of two injections is an injection. So, since there exist injections $A \rightarrow B$ and $B \rightarrow C$, there exists an injection $A \rightarrow C$. Since there also exists an injection $C \rightarrow A$, there exists a bijection $C \rightarrow A$. Similar arguments show the existence of the other required bijections.

4: Write $\Pi = \{p_1, p_2, \dots\}$ with $p_1 < p_2 < \dots$. There is an injection $f : \mathcal{P} \rightarrow \mathbb{N}$ such that, given $X \in \mathcal{P}$, then $f(X)$ is the product of those p_i satisfying $i \in X$. There is an injection $\mathbb{N} \rightarrow \mathcal{P}$ given by $n \mapsto \{n\}$. By the Schröder–Bernstein Theorem, there exists a bijection $\mathbb{N} \rightarrow \mathcal{P}$.

Comment 4.1: A few people gave a very nice argument, without using the assumption about Π . Simply, there is a bijection $f : \mathcal{P} \rightarrow \mathbb{N}$, namely,

$$f(X) = \sum_{x \in X} 2^x .$$

Comments on Midterm 1 solutions

Question 1:

1.1: *Transitivity:*

$$x = (a, \alpha), y = (b, \beta), z = (c, \gamma).$$

$$x \sim y \rightarrow a - b + 2(\alpha - \beta) = 0$$

$$y \sim z \rightarrow b - c + 2(\beta - \gamma) = 0$$

$$a - b + 2(\alpha - \beta) = 0$$

$$a - c + 2(\alpha - \gamma) = 0.$$

$$x \sim z = a - c + 2(\alpha - \gamma) = 0.$$

So transitivity is satisfied too.

Comment: I subtracted only 1 mark, because most of the work is done and the only part left for the reader is to guess the logical status of each statement. But, in more complicated and subtle mathematics, the above style is useless, because the logical status of each statement becomes impossible for the reader to guess.

A few words for expressing a premise:

let, assume, suppose.

A few words for expressing a deduction:

so, hence, therefore.

You absolutely must learn the meanings of these words, otherwise you will not be able to understand much abstract mathematical text. And you absolutely must learn to use them, otherwise you will not be able to communicate substantial abstract mathematics.

If you are at all unsure of how to use those words, you can start with an English-Turkish dictionary, but even a good one may be misleading. You should also consult a good English-English dictionary. Of course, you will also refine your understanding from context, but first make sure you know the literal meanings. Later, you can pick up the way those synonyms differ in nuance.

A simple correction would be:

Let $x = (a, \alpha)$, $y = (b, \beta)$, $z = (c, \gamma)$ be elements of $\mathbb{N} \times \mathbb{N}$.

Assume $x \sim y$ and $y \sim z$.

Then $a - b + 2(\alpha - \beta) = 0$ and $a - c + 2(\alpha - \gamma) = 0$.

So $a - c + 2(\alpha - \gamma) = 0$.

So $x \sim z$. So transitivity is satisfied too.

A more flowing correction would be:

We now show transitivity. Let $x, y, z \in \mathbb{N} \times \mathbb{N}$ and write $x = (a, \alpha)$ and $y = (b, \beta)$ and $z = (c, \gamma)$. Assume $x \sim y$ and $y \sim z$, in other words, $a - b + 2(\alpha - \beta) = 0$ and $a - c + 2(\alpha - \gamma) = 0$. Then $a - c + 2(\alpha - \gamma) = 0$, in other words, $x \sim z$, as required for transitivity.

Question 3: In part (a), you were warned that this is a standard proposition and that you were to provide a proof. You may not assume any reformulation of the same proposition. That would amount to a circular argument.

We defined $|A| \leq |B|$ to mean that there exists an injection $A \rightarrow B$. So the proposition says that $|A| \leq |B|$ if and only if there is a surjection $B \rightarrow A$. But you still have to prove it.

3.1: *If $A \rightarrow B$ is injective then $B \rightarrow A$ is surjective.*

Comment: Many students used this kind of phrasing. It is meaningless. The expression $A \rightarrow B$ is a shorthand for “from A to B ”, which cannot serve as a noun.

There is a yellow coach from Ankara to Beijing. There are also some coaches from Ankara to Beijing that are not yellow. It does not make sense to say “From Ankara to Beijing is yellow”.

The correct statement is about functions, and it has quantifiers: *if there exists an injection f from A to B then there exists a surjection g from B to A .* To prove it, we show that, given such f , then we can define suitable g . For instance, given f , then we can define g to be any tiger that loves f . Actually, that is a poor argument, one objection being that tigers are just not the kind of thing that can be surjective, but at least that argument does have nouns in the places where nouns are needed.

3.2: *If there exist a surjection $B \rightarrow A$ then, for any $a \in A$ there exists at least one $b \in B$. So it means $|B| \geq |A|$ must hold. For $A \rightarrow B$ be injective, for any $b \in B$, there must be at least one $a \in A$ which means that $|A| \leq |B|$.*

Comment: The student does know roughly what he or she wishes to say, but there is too much missing information for the reader to understand it. There exists one $b \in B$ such that what?

Assume there is a surjection $B \rightarrow A$. We ought to name a surjection $B \rightarrow A$. Let us call it g . There exists at least one $b \in B$ such that $a = g(b)$. We must show that there is an injection $A \rightarrow B$. We ought to name such an injection. Let us call it f . How are we to define f in terms of g ? The following definition will work: for each $a \in A$, we define the function f such that $f(a) = b$ where b is a choice of element of B such that $g(b) = a$. Now that we have defined the function f , it is obvious that f is injective. We have deduced that there is an injection $A \rightarrow B$.

Next, we have to go in the opposite direction. Suppose there exists an injection $f : A \rightarrow B$. How are we to define a surjection $g : B \rightarrow A$ in terms of f ? Given $b \in \text{im}(f)$, say $b = f(a)$, then we can define $g(b) = a$. But that definition of g is not complete, because we still have to deal with the possibility that some elements of b are not in $\text{im}(f)$.

Evidently, that standard proposition in part (a) is not trivial. It does have some content. You were being asked to supply that content.

3.3: *Statement of theorem: If there is an injection $X \rightarrow Y$ and there is an injection $Y \rightarrow X$, then there is a bijection $X \rightarrow Y$.*

Comment: What are X and Y ? The above just records the conclusion of the theorem. What is the hypothesis? The hypothesis of the theorem is that X and Y are sets.

MATH 123: Abstract Mathematics 1



Midterm 1 Retake

4 December 2024, Laurence Barker

The duration of the exam is 120 minutes.

All 5 questions have equal weight.

Eligibility for the retake is (a) a Midterm 1 mark of less than 50 percent, (b) office discussion concerning your Midterm 1 paper. If you score more than 50 in this exam, your course credit mark will be recorded as 50.

Please write your name clearly on every sheet of your script.

If you do not write in complete sentences, the examiner will still try to understand what you are saying. But you are strongly advised to write in complete sentences, because that will probably help the examiner understand what you are saying.

No notes or texts may be used during the exam, nor electronic devices, nor red pens, nor very faint pencils.

Do take the question sheet home. No writing on handed in question sheets will be marked.

1: Let A and B be sets and let F be the set of functions $A \rightarrow B$. We define a relation $\sim$ on F such that, given $f, g \in F$, then $f \sim g$ if and only if there exist bijections $\alpha : A \rightarrow A$ and $\beta : B \rightarrow B$ satisfying $f \circ \alpha = \beta \circ g$. Is $\sim$ an equivalence relation?

2: Let $M = \{1, 2, 3, 4, 5\}$ and $N = \{1, 2, 3\}$.

(a) How many functions $M \rightarrow N$ are there?

(b) State a formula for the size of the union of 3 finite sets, then use it to obtain a formula for the number of surjections $M \rightarrow N$.

(c) How many surjections $f : M \rightarrow N$ are there such that $f(1) = 1$?

(d) How many surjections $f : M \rightarrow N$ are there such that $f(1) = 1$ and $f(2) = 2$?

(e) How many surjections $f : M \rightarrow N$ are there such that $f(1) = 1$ and $f(2) = 2$ and $f(3) = 3$?

3: Let r and s be positive real numbers. Let

$$U(r) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 < r^2\}, \quad V(s) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq s^2\}.$$

(a) Give a geometric description of the sets $U(r)$ and $V(s)$.

(b) Without mentioning the cardinal numbers, show that there is a bijection $U(r) \rightarrow V(s)$.

4: State and prove Cantor's Theorem (concerning the power set of a given set).

5: Let $\mathcal{S}$ be the set of infinite sequences of natural numbers. Let $\mathcal{F}$ be the set of functions $\mathbb{N} \rightarrow \mathbb{N}$. In terms of the relations $=$ and $\leq$ on the cardinal numbers, compare the cardinal numbers $|\mathcal{P}(\mathbb{N})|$ and $|\mathcal{S}|$ and $|\mathcal{F}|$.

Solutions to Midterm 1 Retake

1: Let $f, g, h \in F$. We have $f \circ \text{id}_A = \text{id}_B \circ f$, so $f \sim f$. Thus, $\sim$ is reflexive. Plainly, $\sim$ is symmetric. Suppose $f \sim g$ and $g \sim h$, say $f \circ \alpha = \beta \circ g$ and $g \circ \gamma = \delta \circ h$ for bijections $\alpha, \beta, \gamma, \delta$. Then $\alpha \circ \gamma$ and $\beta \circ \delta$ are bijections, also $f \circ \alpha \circ \gamma = \beta \circ \delta \circ h$. Therefore, $f \sim h$. Thus, $\sim$ is transitive. We have shown that $\sim$ is an equivalence relation.

2: Part (a). Of course, the answer is $3^5 = 243$.

Part (b). Given finite sets P, Q, R then

$$|P \cup Q \cup R| = |P| + |Q| + |R| - |Q \cap R| - |P \cap R| - |P \cap Q| + |P \cap Q \cap R|.$$

For each $i \in \{1, 2, 3\}$, let S_i be the set of functions $f : M \rightarrow N$ such that i is not a value of f . We have $|S_i| = 2^5$. For $i \neq j$, we have $|S_i \cap S_j| = 1$. Also, $|S_1 \cap S_2 \cap S_3| = 0$. Applying the above formula with S_1, S_2, S_3 in place of P, Q, R , we deduce that

$$|S_1 \cap S_2 \cap S_3| = 3|S_1| - 3|S_1 \cap S_2| = 3 \cdot 2^5 - 3 = 3 \cdot 31.$$

So the number of surjections $M \rightarrow N$ is

$$3^5 - |S_1 \cap S_2 \cap S_3| = 3 \cdot (81 - 31) = 3 \cdot 50 = 150.$$

Part (c). One third of the surjections satisfy $f(1) = 1$, so the answer is $150/3 = 50$.

Part (d). Consider the functions $f : M \rightarrow N$ satisfying $f(1) = 1$ and $f(2) = 2$. For each such f , let $\bar{f}$ be the restriction of f to a function $\{3, 4, 5\} \rightarrow N$. The number of such f is the number of $\bar{f}$, which is $3^3 = 27$. The number k of non-surjective f is the number of those $\bar{f}$ that do not have value 3. So $k = 2^3 = 8$. The answer is $27 - 8 = 19$.

Part (e). The condition on f now guarantees surjectivity. By restricting the specified f to functions $\{4, 5\} \rightarrow N$, we see that the answer is $3^2 = 9$.

3: Part (a). By Pythagoras' Theorem, $U(r)$ is the set of points of the plane $\mathbb{R} \times \mathbb{R}$ that are inside the circle with centre $(0, 0)$ and radius r . Likewise, $V(s)$ is the set of points inside or on the circle with centre $(0, 0)$ and radius s .

Part (b). There is an injection $U(r) \rightarrow V(s)$ given by $(x, y) \mapsto (xs/r, ys/r)$. There is an injection $V(s) \rightarrow U(r)$ given by $(x, y) \mapsto (xr/2s, yr/2s)$. The required conclusion now follows by the Bernstein–Schröder Theorem.

4: Cantor's Theorem: Given a set S , then there is no surjection $S \rightarrow \mathcal{P}(S)$.

Proof: For a contradiction, consider a surjection $f : S \rightarrow \mathcal{P}(S)$. Let $T = \{s \in S : s \notin f(s)\}$. By the hypothesis on f , there exists $t \in S$ such that $T = f(t)$. We have arrived at a contradiction, because if $t \in T$, then the definitions of t and T yield $t \notin T$, whereas if $t \notin T$, then those definitions yield $t \in T$. $\square$

5: There is a bijection $\mathcal{F} \rightarrow \mathcal{S}$ given by $f \mapsto (f(0), f(1), \dots)$. So $|\mathcal{S}| = |\mathcal{F}|$. There is an injection $\mathcal{P}(\mathbb{N}) \rightarrow \mathcal{S}$ given by $X \mapsto (x_0, x_1, \dots)$ where $x_i = 1$ if and only if $i \in X$. So $|\mathcal{P}(\mathbb{N})| \leq |\mathcal{S}|$. There is an injection $\mathcal{S} \rightarrow |\mathcal{P}(\mathbb{N})|$ such that $(y_0, y_1, \dots) \mapsto \{z_0, z_1, \dots\}$ where $z_0 = y_0$ and each $z_{n+1} = z_n + y_{n+1} + 1$. So $|\mathcal{P}(\mathbb{N})| \geq |\mathcal{S}|$. In conclusion, $|\mathcal{P}(\mathbb{N})| = |\mathcal{S}| = |\mathcal{F}|$.

MATH 123: Abstract Mathematics 1

Midterm 2

9 December 2024, Laurence Barker



The duration of the exam is 120 minutes.

Please write your name clearly on every sheet of your script.

No notes or texts may be used during the exam, nor electronic devices, nor red pens, nor very faint pencils.

Do take the question sheet home. No writing on handed in question sheets will be marked.

Reminder: Justify your answers.

Reminder: “Let X be a fish” means that we are introducing X and we are to assume that X is a fish. We may not assume that X is our favorite fish.

1: (20 marks.) Give a complete definition of the notion of an equivalence relation. You may assume that the reader knows what a set is and what a relation is.

Warning: Write it out fully, with all the necessary quantifiers, all your terms properly introduced. Do not assume that the reader already knows the answer. The following kind of answer, which is not even arranged in sentences, would score zero marks:

reflexivity $x \sim x$, *symmetry* $x \sim y, y \sim x$, *transitivity* $x \sim y, y \sim z, x \sim z$.

2: (20 marks.) Find integers u and v such that $\gcd(3241, 2975) = 3241u + 2975v$.

3: (20 marks.) Let α and β be distinct nonzero real numbers. Let $b = -(\alpha + \beta)$ and $c = \alpha\beta$. Let $x_0, x_1, \dots$ be a sequence of real numbers such that

$$x_{n+2} + bx_{n+1} + cx_n = 0$$

for all natural numbers n .

(a) Prove that there exist real numbers A and B such that, for all $n \in \mathbb{N}$, we have

$$x_n = A\alpha^n + B\beta^n.$$

(Warning: This is a well-known result, but you are required to prove it.)

(b) Give a counter-example to show that, if we remove the condition that α and β are distinct, then the conclusion of (a) may fail.

4: (20 marks.) Let p be a prime number.

(a) State, without proof, a theorem concerning the inverse of a nonzero element of $\mathbb{Z}/p$.

(b) State and prove Wilson’s Theorem concerning $(p - 1)!$ modulo p .

(c) For which positive integers n is $(n - 1)!$ divisible by n ? (Remember to justify your answer.)

5: (20 marks.) Let p, q, r be mutually distinct prime numbers and let a, b, c be positive integers. Let $n = p^a q^b r^c$. Give a formula for the number of integers m in the range $0 < m < n$ such that $\gcd(m, n) = 1$. (Remember to justify your answer.)

Solutions to Midterm 1

1: An equivalence relation on a set X is a relation $\equiv$ such that the following three conditions hold. Reflexivity: for all $x \in X$, we have $x \equiv x$. Symmetry: for all $x, y \in X$ such that $x \equiv y$, we have $y \equiv x$. Transitivity: for all $x, y, z \in X$ such that $x \equiv y$ and $y \equiv z$, we have $x \equiv z$.

Comment 1: Using a standard logical notation, the three conditions can be expressed as:

Reflexivity: $(\forall x \in X)(x \equiv x)$.

Symmetry: $(\forall x, y \in X : x \equiv y)(y \equiv x)$.

Transitivity: $(\forall x, y, z \in X : (x \equiv y) \wedge (y \equiv z))(x \equiv z)$.

Comment 2: The overwhelming majority got this easy question right, but a few are still displaying misconceptions of the nature of present day mathematical culture.

(1) “When we want to show the equivalence relation reflexivity between $x \sim x$ in a given function we put the values $\{a, b\}$ for the variables and then compare the answers.”

(2) “Suppose that $x \sim x$ is reflexive. Let $x = (a, \alpha)$ and $y = (b, \beta)$. Then $x \sim y$ and $y \sim x$ are symmetric. ... So the above terms which are reflexivity, symmetry and transitivity proves the notion of an equivalence relation.”

These are, at least, grammatically well-written sentences. So some progress has been made. The problem now is with the meaning, the content. A motorbike is when we want to get to Istanbul? No, a motorbike is not a situation that demands some action. A motorbike is a motorized bicycle with an engine powerful enough to break motorway speed limits. In particular, a motorbike is a particular kind of object.

Likewise, an equivalence relation is not a situation that requires us to do something. It has nothing to do with our desires “When we want ...”, nothing to do with our thoughts “Suppose that ...”, nothing to do with any kind of human activity. An equivalence relation is a particular kind of object. An equivalence relation is a relation that satisfies three conditions called reflexivity, symmetry, transitivity. To complete the response to the question, we must also define those three conditions.

2: We have

$$3241 = 1.2975 + 266 .$$

Since $11.166 = 2926$, we have

$$2975 = 11.266 + 49 .$$

We have $266 = 5.49 + 21$. Also, $49 = 2.21 + 7$ and $7 = 3.7$. So $\gcd(3241, 2975) = 7$. Now

$$\begin{aligned} 7 &= 49 - 2.21 = 49 - 2(266 - 5.49) = 11.49 - 2.266 = 11(2975 - 11.266) - 2.266 \\ &= 11.2975 - 123.266 = 11.2975 - 123(3241 - 2975) = 134.2975 - 123.3241 . \end{aligned}$$

So we can take the Bézout coefficients to be $u = -123$ and $v = 134$.

3: Part (a). It is easy to see that, since $\alpha \neq \beta$, there exist A and B such that $x_0 = A + B$ and $x_1 = A\alpha + B\beta$. Let $y_n = A\alpha^n + B\beta^n$. Then $x_0 = y_0$ and $x_1 = y_1$. Now suppose, inductively, that $x_n = y_n$ and $x_{n+1} = y_{n+1}$. We have

$$\alpha^2 + b\alpha + c = \alpha^2 - (\alpha + \beta)\alpha + \alpha\beta = 0$$

and similarly for β . So

$$y_{n+2} + by_{n+1} + cy_n = A\alpha^n(\alpha^2 + b\alpha + c) + B\beta^n(\beta^2 + b\beta + c) = 0 = x_{n+2} + bx_{n+1} + cx_n .$$

By the inductive assumption, $by_{n+1} + cy_n = bx_{n+1} + cx_n$. We deduce that $y_{n+2} = x_{n+2}$. $\square$

Part (b). Put $\alpha = \beta = 1$. Then the sequence given by $x_n = n$ satisfied the hypothesis but not the conclusion.

Alternative solution for part (a): Let A and B be as determined by the equalities in the cases $n = 0$ and $n = 1$. Let $y_n = A\alpha^n + B\beta^n$. For a contradiction, let n be minimal such that $x_n \neq y_n$. Trivially, $n \geq 2$. By direct calculation,

$$y_n + by_{n-1} + cy_{n-2} = A\alpha^{n-2}(\alpha^2 + b\alpha + c) + B\beta^{n-2}(\beta^2 + b\beta + c) = 0 = x_n + bx_{n-1} + cx_{n-2} .$$

Since $x_n \neq y_n$, we have $x_{n-1} \neq y_{n-1}$ or $x_{n-2} \neq y_{n-2}$, contradicting the minimality of n . $\square$

Another alternative solution: Put

$$A = \frac{\beta x_0 - x_1}{\beta - \alpha} , \quad B = \frac{\alpha x_0 - x_1}{\alpha - \beta} .$$

Let $y_n = A\alpha^n + B\beta^n$. We have $y_0 = A + B = x_0$ and $y_1 = A\alpha + B\beta = x_1$. Now

$$t^2 + bt + c = (t - \alpha)(t - \beta)$$

for all $t \in \mathbb{R}$. Perforce, $\alpha^2 + b\alpha + c = 0 = \beta^2 + b\beta + c$. So, by direct calculation,

$$y_{n+2} + by_{n+1} + cy_n = 0 .$$

The infinite sequence $(x_0, x_1, \dots)$ is determined by x_0 and x_1 together with the recurrence equation. So $(y_0, y_1, \dots) = (x_0, x_1, \dots)$. $\square$

Comment 1: The manipulations of formulas in this question are easy, the kind of routine that everyone learned to do at school. The logic is not so straightforward.

The aim in part (a) was to show that such A and B exist. Many examinees completely disregarded the logic by treating A and B as if they were given, putting $x_n = A\alpha^n + B\beta^n$, then calculating

$$\begin{aligned} x_{n+2} + bx_{n+1} + cx_n &= A\alpha^{n+2} + B\alpha^{n+2} + A\alpha^{n+2} + B\alpha^{n+2} + A\alpha^n + B\alpha^n \\ &= A\alpha^n(\alpha^2 - (\alpha + \beta)\alpha + \alpha\beta) + B\beta^n(\beta^2 - (\alpha + \beta)\beta + \alpha\beta) = 0 \end{aligned}$$

finally concluding that the solution had been confirmed.

By that is deduction in the wrong direction. It shows that the required conclusion implies the specified hypothesis. What we should be doing is to show that the hypothesis implies the conclusion.

That backwards argument would be no less valid if one were to put $x_n = 0$ for all n .

The point of part (b) was to warn you that the argument must break down when we drop the condition that $\alpha \neq \beta$. Thus, if your answer to part (a) did not use the condition $\alpha \neq \beta$, then your argument must be wrong.

Let us look at what happens in the situation of part (b) when we run through the backwards argument. Suppose $\alpha = \beta$, in other words, $b = -2\alpha$ and $c = \alpha^2$. If we assume that $x_n = A\alpha^n$ for all n , then a straightforward calculation shows that $x_{n+2} + bx_{n+1} + cx_n = 0$ for all n . But,

as the above counter-example reveals, the recurrence equation $x_{n+2} + bx_{n+1} + cx_n$ has other solutions.

A further exercise in the same techniques: Supposing $\alpha = \beta$, show that there exist real numbers C and D such that, for all n , we have $x_n = (C + Dn)\alpha^n$.

Comment 2: The hardest bit of part (a) was the base step. In one of the above three solutions, a formula is given for A and B . To find that formula, I considered the equation $\alpha x_0 = \alpha A + \alpha B$, then I subtracted the equation for x_1 . But that working had to be omitted from the proof. It cannot be a legitimate part of the proof since it presupposes the desired conclusion, namely, the existence of A and B . This is not “show all your reasoning” school mathematics. This is “Show only your final deductive argument” university mathematics.

4: Part (a). Every nonzero element of $\mathbb{Z}/p$ has an inverse.

Part (b). Wilson’s Theorem asserts that $(p-1)! \equiv_p -1$.

To prove it, we first note that the case $p = 2$ is trivial. So we may assume that $p \neq 2$. For all $x \in \mathbb{Z}/p$, we have $x^2 - 1 = (x-1)(x+1)$. So $x^{-1} = x$ if and only if $x = [1]$ or $x = [-1]$. All the terms of the product $[1][2]\dots[p-1]$ cancel with their inverse except for the first term $[1]$ and the last term $[p-1] = [-1]$, so $[(p-1)!] = [1][-1] = [-1]$. $\square$

Part (c). We shall show that a positive $(n-1)!$ is divisible by n if and only if n is not prime and $n \neq 4$. This is clear when n is prime or $n = 4$. It is also clear when $n = 1$ or $n = p^2$ for an odd prime p . It remains only to deal with the case where $n = ab$ for distinct integers $a > 1 < b$. In that case, a and b both appear as terms in the product $(n-1)!$, hence n divides $(n-1)!$.

5: Let k be the number of m as specified. Let $X = \{1, \dots, n\}$. Let P, Q, R , respectively, be the set of elements of X that are divisible by p, q, r . Noting that $n \in P \cup Q \cup R$, we have

$$k = |X| - |P \cup Q \cup R|.$$

We have $|P| = n/p$ and $|Q| = n/q$ and $|R| = n/r$. Also,

$$|P \cap Q| = n/pq, \quad |P \cap R| = n/pr, \quad |Q \cap R| = n/qr.$$

Also, $|P \cap Q \cap R| = n/pqr$. Using the inclusion-exclusion formula

$$|P \cup Q \cup R| = n(1/p + 1/q + 1/r - 1/pq - 1/pr - 1/qr + 1/pqr).$$

We have $|X| = n$. Therefore, $k = n(1 - 1/p)(1 - 1/q)(1 - 1/r)$.

Comment: The **Euler function** ϕ is defined to be such that,

$$\phi(n) = |\{[a] \in \mathbb{Z}/n : \gcd(a, n) = 1\}|.$$

Note that $\gcd(a, n)$ is well-defined for $[a] \in \mathbb{Z}/n$. We have not covered the Inclusion-Exclusion Formula for the size of the union of finitely many finite sets. But we mention that the argument above generalizes to a proof that, for any positive integer n , we have

$$\phi(n) = \prod_p (1 - 1/p) = \prod_p (p-1)/p$$

where p runs over the prime factors of n .

MATH 123: Abstract Mathematics 1

Final

3 January 2025, Laurence Barker



The duration of the exam is 120 minutes.

Please write your name clearly on every sheet of your script.

No notes or texts may be used during the exam, nor electronic devices, nor red pens, nor very faint pencils.

Do take the question sheet home. No writing on handed in question sheets will be marked.

Reminder: Justify your answers.

1: (25 marks.) Let n be an integer with $n \geq 2$. Consider the ring of modulo n congruence classes

$$\mathbb{Z}/n = \{[x]_n : x \in \mathbb{Z}\}.$$

(a) Define the usual addition operation on $\mathbb{Z}/n$ and show that it is well-defined.

(b) Define the usual multiplication operation on $\mathbb{Z}/n$ and show that it is well-defined.

2: (25 marks.) Let $\mathcal{C}$ be a commutative ring with an element n such that $n^2 = 0$ and each element of $\mathcal{C}$ can be expressed uniquely in the form $x + ny$ where x and y are rational numbers. The addition and multiplication in $\mathcal{C}$ are given by

$$x + ny + x' + ny' = x + x' + n(y + y'), \quad (x + ny)(x' + ny') = xx' + n(xy' + yx').$$

Find all the ideals of $\mathcal{C}$.

3: (25 marks.) You may not make use of the real numbers in this question, which is about the construction of the real numbers.

(a) Define the term **Cauchy sequence of rational numbers**. (Just give the definition. There are no marks for discussion.)

(b) In the construction of the real numbers, what is the definition of **equivalence** of Cauchy sequences of rational numbers? (Just give the definition.)

(c) Prove that the relation you defined in part (b) is an equivalence relation.

4: (25 marks.) Let a be a positive integer and $n = 2^a$. Find all the elements x of $\mathbb{Z}/n$ such that $x^4 = [1]_n$. (Hint: deal with the three cases $a = 1$ and $a = 2$ and $a \geq 3$ separately.)

Solutions to Final

1: Part (a). The addition is defined by $[x] + [y] = [x + y]$ for $x, y \in \mathbb{Z}$. Given $x', y' \in \mathbb{Z}$ such that $[x'] = [x]$ and $[y'] = [y]$, then $x' = x + nu$ and $y' = y + nv$ for some $u, v \in \mathbb{Z}$. We have $x' + y' = x + y + n(x' + y')$, so $[x' + y'] = [x + y]$ and the addition is well-defined.

Part (b). The multiplication is defined by $[x][y] = [xy]$. Let x' and y' be as above. Then $x'y' = xy + n(uy + vx + nuv)$, hence $[x'y'] = [xy]$ and the multiplication is well-defined.

2: We shall show that the ideals of $\mathcal{C}$ are $\{0\}$ and $\mathcal{C}$ and $\mathcal{N} = \{nz : z \in \mathbb{Z}\}$. First note that, since the identity element of $\mathcal{C}$ is $1 = 1 + n0$, we can regard $\mathbb{Q}$ as a subring of $\mathcal{C}$ and there is a bijective correspondence $\mathbb{Q} \times \mathbb{Q} \leftrightarrow \mathcal{C}$ given by $(x, y) \leftrightarrow x + ny$. Let I be an ideal of $\mathcal{C}$ such that $I \neq \{0\}$ and $I \neq \mathcal{C}$. Let $a = x + iy$ be a nonzero element of I . For a contradiction, suppose $x \neq 0$. Then a is invertible, indeed, $a^{-1} = (x - ny)/x^2$. Hence $1 \in I$ and $I = \mathcal{C}$, which is a contradiction. We deduce that $a = ny$ with $y \neq 0$. So $I \subseteq \mathcal{N}$. Given $nz \in \mathcal{N}$, then $nz = ny(z/y) \in I$. We conclude that $I = \mathcal{N}$.

3: Part (a). A **Cauchy sequence of rational numbers** is a sequence $\underline{x} = (x_0, x_1, \dots)$ such that, for all positive rational ϵ , we have $|x_m - x_n| < \epsilon$ for all sufficiently large m and n .

Part (b). Two Cauchy sequences of rationals $\underline{x}$ and $\underline{y}$ are **equivalent** provided, for all positive rational ϵ , we have $|x_n - y_n| < \epsilon$ for all sufficiently large n .

Part (c). Let $\equiv$ denote the relation defined in part (b). The reflexivity and symmetry of $\equiv$ are obvious. Let $\underline{x}, \underline{y}, \underline{z}$ be Cauchy sequences of rationals. Let ϵ be a positive rational. For all sufficiently large n , we have $|x_n - y_n| < \epsilon/2 < |y_n - z_n|$. By the Triangle Inequality, $|x_n - z_n| = |x_n - y_n + y_n - z_n| \leq |x_n - y_n| + |y_n - z_n| < \epsilon/2 + \epsilon/2 = \epsilon$.

4: It is easy to check that, when $a \leq 4$, the solutions to $x^4 = 1$ are the elements $[z]$ where z is odd. We shall show that, for $a \geq 4$, there are precisely 8 solutions to $x^4 = [1]$, namely $x = [m2^{a-2} \pm 1]$ where $m \in \mathbb{Z}$. It is easy to check that all of those cases are solutions. We must show that there are no others. For a contradiction, let a be minimal such that there is some other solution x . Then $a \geq 5$. By the minimality of a , we have $x = [z]$ where

$$z = m2^{a-3} \pm 1$$

and m is odd. Then

$$z^4 = m^4 2^{4a-12} \pm 4m^3 2^{3a-9} + 6m^2 2^{2a-6} \pm 4m 2^{a-3} + 1 \equiv_n 2^{a-1} + 1 \not\equiv_n 1$$

which is a contradiction, as required.