

Archive for
MATH 124, Abstract Mathematics 2, Spring 2025

Bilkent University, Laurence Barker, 11 June 2025

Source file: arch124spr25.tex

page 2: Course specification.

page 5: Homeworks.

page 10: Quizzes.

page 13: Midterm 1.

page 14: Solutions to Midterm 1.

page 15: Midterm 2.

page 16: Solutions to Midterm 2.

page 17: Final.

page 18: Solutions to Final.

Course specification

MATH 124, *Abstract Mathematics 2*, Spring 2025

Laurence Barker, Bilkent University. Version: 9 March 2025.

Course Aims: The purpose of the course is to give an introductory taste of abstract mathematics, that is, the conceptual study of structures as opposed to formal procedural technique. Specifically, it is to introduce enough algebra to yield some applications to classical number theory, enough real analysis to yield some basics concerning continuous functions. It is not the purpose of the course to present full integral account to any single area of study; that will be for subsequent courses.

Course Description: This course will differ from MATH 123 in that a basic grasp of a mathematical mode of discussion will be presumed in class. Backtracking over the preliminaries is to be done in office hours. Most of the tranches of material will be taken from early chapters of textbooks on specific areas of mathematics.

Course Requirements: Basic knowledge of sets, functions, equivalence relations, mathematical induction. Ability to interpret mathematical statements and to write mathematical statements.

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

Assistant: Cazibe Kavalci, kazibekavalci at gmail dot com.

Texts:

Required textbook:

- Stephen G. Krantz, “The Elements of Advanced Mathematics”, 4th edition, (CRC Press, 2017).

Recommended texts:

- Sheldon Axler, “Linear Algebra Done Right”, 4th edition, (Springer, 2024).
- Robert G. Bartle, Donald R. Sherbert, “Introduction to Real Analysis”, 3rd edition, (Wiley, 2000).
- David M. Burton, “Elementary Number Theory”, 7th edition, (McGraw–Hill, 2010).
- Keith Devlin, “The Joy of Sets”, (Springer, 1993).
- David S. Dummit, Richard M. Foote, “Abstract Algebra”, 3rd edition, (Wiley, 2004).
- Stephen Galovich, “Introduction to Mathematical Structures”, (Harcourt Brace Jovanovich, 1989).

See also supplementary material on my homepage

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

and on Moodle.

Specific Chapters:

- *General preliminaries:* Krantz: set theory Chapter 5; real numbers Chapter 6; number theory Chapter 9; group theory Chapter 11.
- *Groups and rings:* Dummit–Foote Chapters 1, 2, 3, 7.
- *Matrices:* Axler, Chapter 3.
- *Euler function, sums of squares:* Burton, Chapters 7, 13.
- *ZF axioms, natural numbers, Zorn’s Lemma:* Devlin, Chapter 2.
- *Cantor’s Construction of the reals:* Galovich, Chapter 7.
- *Sequences, limits, continuous functions:* Bartle–Sherbert, Chapters 3, 4, 5.

Classes: Tuesdays 10:30 - 12:20, Thursdays 15:30 - 17:20, room FF-B06.

Office Hours: Tuesdays, 12:30 - 13:20 in my office, room SA-129 (or sometimes in FF-B06).

Weekly Syllabus

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

- 1:** 27 Jan: Groups, isomorphism, subgroups, Lagrange’s Theorem. Euler’s totient function.
- 2:** 3 Feb: Normal subgroups, quotient groups, First Isomorphism Theorem.
- 3:** 10 Feb: Rings, ideals, quotient rings. Matrix rings.
- 4:** 17 Feb: Construction of the complex numbers and quaternions. Sums of squares.
- 5:** 24 Feb: The ZF axioms.
- 6:** 3 Mar: Partial orderings. Well orderings.
- 7:** 10 Mar, *only Thursday:* Construction of the natural numbers.
- 8:** 17 Mar: Zorn’s Lemma, with applications.
- 9:** 24 Mar: Cauchy sequences
- 10:** 31 Mar, *only Thursday:* Construction of the reals. Limits.
- 11:** 7 Apr: Completeness of the reals.
- 12:** 14 Apr: Bolzano–Weierstrauss Theorem.
- 13:** 21 Apr: Continuous functions. Intermediate value Theorem.
- 14:** 28 Apr, *only Tuesday:* Topological spaces.
- 15:** 5 May: Review or optional topic.
- 16:** 12 May, *only Tuesday:* Review for Final Exam.

Assessment:

A minimum of 75% attendance is required.

- Quizzes 10%.
- Midterm 1, 25%, Monday, 17 March, 19:30 - 21:30, [rooms to be announced].
- Midterm 2, 30%, Monday, 14 April, 19:30 - 21:30, [rooms to be announced].
- Final, 35%.

FZ criteria: Failure to attend classes, or failure to attend midterms, or average score of less than 20 percent in the midterms.

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.

Homework

MATH 124, *Abstract Mathematics 2*, Spring 2025, Laurence Barker

version: 12 April 2025

Credit for homework will accrue in the following indirect way: Doing the homework will make you better at mathematics. In particular, experience with the homework will be useful in the quizzes and very useful in the exams.

Tip for those struggling: the basic question is not: *What must I do here?* The basic question is: *What does this mean and why is it true?*

Solutions to the homework will mostly be presented in class and in office hours.

Homework 1:

Exercise 1.1: Read Dummit–Foote Section 1.1.

Exercise 1.2: Make sure you understand the last statement made in class on 28 January: *The groups $(\mathbb{Z}/4, +)$ and $((\mathbb{Z}/5)^\times, \cdot)$ are isomorphic.* That statement has several different concepts packed into it. Understanding that kind of statement is important.

Exercise 1.3: Do the following exercises from Dummit–Foote pages 21 to 23: numbers 9, 12, 21, 25, 31, 36. (Warning: You should be able to do this exercise. If you are having trouble, do Exercise 1.1 again, slowly and carefully.)

Quiz 1 in Week 2 will be in the style of those Dummit–Foote exercises.

Exercise 1.4, harder: Classify the groups with order 10 up to isomorphism.

Exercise 1.5, yet harder: Classify the groups with order 8 up to isomorphism.

Homework 2:

Exercise 2.1: Read Dummit–Foote Sections 3.1, 3.2, 3.3, focussing on what has been covered in class.

Exercise 2.2: Do D–F Exercise 3.2.9, proof of Cauchy’s Theorem.

Exercise 2.3: As in D–F Exercise 3.2.12, show that, for any subgroup H of a group G , the set of left cosets of H in G has the same cardinality as the set of right cosets of H in G .

Exercise 2.4: Do D–F exercises 3.3.4, 3.3.7.

Exercise 2.5: Let G be a group and let A and B be normal subgroups of G such that G/A and G/B are abelian. By considering a homomorphism $G \rightarrow G/A \times G/B$, show that $G/(A \cap B)$ is abelian.

Homework 3:

Exercise 3.1: Do the introductory ring theory D–F Exercises 7.1.1, 7.1.2, 7.1.3, 7.1.7, 7.1.8.

Exercise 3.2: Find all the square roots of -1 in the ring of quaternions $\mathbb{H}$.

Recall, a **unit** of a ring R is an element of R with an inverse.

Exercise 3.3: Let

$$R = \left\{ \begin{bmatrix} x & y \\ 0 & x \end{bmatrix} \mid x, y \in \mathbb{R} \right\}$$

as a subring of $\text{Mat}_2(\mathbb{R})$. Find all the units in R .

Exercise 3.4: Let $S = \mathbb{R} \times \mathbb{R}$ as a ring where addition and multiplication are given by

$$(x, y) + (\xi, \eta) = (x + \xi, y + \eta), \quad (x, y)(\xi, \eta) = (x\xi, x\eta + y\xi).$$

Find all the units in S .

The following exercise came up in discussion during office hours. Some background is needed, as follows. Given a set X , then a bijection $X \rightarrow X$ is called a **permutation** of X . The **symmetric group** on X , denoted $\text{Sym}(X)$, is defined to be the set of permutations of X , with composition of functions as the group operation. Note that, if X is a finite set with size n , then the order of $\text{Sym}(X)$ is

$$|\text{Sym}(X)| = n!.$$

Exercise 3.5: Prove the following theorem:

Picard's Theorem: Let G be a finite group, $H \leq G$ and suppose that $|G|/|H|$ is the smallest prime factor of $|G|$. Then $H \trianglelefteq G$.

Hint: Take X be the set of left cosets of H in G and consider the homomorphism

$$\theta : G \rightarrow \text{Sym}(X)$$

given by $\theta(g)(xH) = gxH$.

Not needed for the above exercise, but we mention that the **symmetric group with degree n** is defined to be

$$S_n = \text{Sym}(\{1, \dots, n\}).$$

The importance of S_n lies in the fact that $S_n \cong \text{Sym}(X)$ where X is any set with size n .

Homework 4:

Exercise 4.1: Find the smallest positive integer x such that $x \equiv_5 2$ and $x \equiv_7 3$ and $x \equiv_{11} 10$.

Exercise 4.2: Read “Notes on Lagrange’s Four Square Theorem” on my homepage and then, following the outline supplied in the notes, prove Euler’s Two squares Theorem.

Homework 5: shortly before Midterm 1.

Exercise 5.1: Find the smallest positive integer z such that $z \equiv_4 6$ and $z \equiv_5 7$ and $z \equiv_7 10$.

Exercise 5.2: Express the following groups, up to isomorphism, as direct products having the form $C_{q_1} \times C_{q_2} \times \dots$ where q_1, q_2 are powers of primes. Examples: $(\mathbb{Z}/8)^\times \cong C_2 \times C_2$ and $C_{13} \cong C_4 \times C_3$.

(a) $(\mathbb{Z}/9)^\times$, (b) $(\mathbb{Z}/16)^\times$, (c) $(\mathbb{Z}/5)^\times$, (d) $(\mathbb{Z}/25)^\times$, (e) $(\mathbb{Z}/30)^\times$.

Exercise 5.3: Let n be a positive integer. Show that the group $(\mathbb{Z}/3^n)$ is cyclic.

Exercise 5.4: What is the smallest positive integer n such that $(\mathbb{Z}/n)^\times$ has a subgroup isomorphic to $C_2 \times C_2 \times C_2$?

Exercise 5.5: Classify, up to isomorphism, the posets with size 5 and height 4.

Exercise 5.6: Let $-1 < r < 1$ and let $\underline{a} = (a_n)$ be a rational sequence such that $|a_n| < r^n$. Show that

- (a) the sequence $\underline{a}$ is a null sequence,
- (b) the sequence (s_n) is a Cauchy sequence, where $s_n = \sum_{i=0}^n a_i$.

Exercise 5.7: Let $\underline{b} = (b_n)$ be a sequence of rational numbers such that each $-1 \leq b_n \leq 1$. Show that some subsequence of $\underline{b}$ is a Cauchy sequence. (A subsequence is obtained from a sequence by deleting some of the terms.)

Exercise 5.8: Consider the subring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

of the ring of 2×2 real matrices.

- (a) Find all the units of R .
- (b) Find all the ideals of R .

Homework 6: shortly before Midterm 2.

Exercise 5.1: Do the exercises on the final page of “Notes on Cantor’s construction of the real number field”.

Homework solutions

3.2: See the solution to Quiz 4.

3.5: Let $K = \ker(\theta)$ and $I = \text{im}(\theta)$. It suffices to show that $H = K$. Plainly, $H \leq K$. So it suffices to show that $|H| = |K|$. Let p be the smallest prime factor of $|G|$. By Lagrange's Theorem, $|I|$ divides $p!$, whereas, by the First Isomorphism Theorem and Lagrange's Theorem again, $|I| = |G|/|K|$ which divides $|G|$. The hypothesis on p implies that $|I| = p$. Therefore, $|H| = |K|$, as required.

4.1: Recall that, to solve simultaneous congruences $x \equiv_{n_i} b_i$, where i runs over some indices, we define $n = \prod_i n_i$ and $m_i = n/n_i$, we let y_i be an inverse of m_i modulo n_i , and we put

$$x = \sum_i y_i m_i b_i .$$

Note that the y_i are well-defined up to congruence modulo n_i and the solution x is well-defined up to congruence modulo n .

In this exercise, $m_1 = 77 \equiv_5 2$ and we can put $y_1 = 2$. We have $m_2 = 55 \equiv_7 6$ and we can put $y_2 = 6$. Also, $m_3 = 35 \equiv_{11} 2$ and we can put $y_3 = 6$. Then

$$x \equiv_n 3.77.2 + 6.55.3 + 6.35.10 = 3552 .$$

We have $n = 5.7.11 = 385$ and $3552 = 9.385 + 87$. So $x = 87$.

4.2: The solution now appears in those notes.

5.1: Put $n_1 = 4$ and $n_2 = 5$ and $n_3 = 7$. Let $n = n_1 n_2 n_3 = 140$. Let $m_i = n/n_i$ and let y_i be an inverse of m_i modulo n_i . Then $m_1 = 35$ and $m_2 = 28$ and $m_3 = 20$. Modulo 4, 5, 7, respectively, some inverses of m_1, m_2, m_3 are $-1, 2, -1$. We are to solve $z \equiv_{n_i} b_i$ where $b_1 = 2$ and $b_2 = 2$ and $b_3 = 3$. A solution is

$$z' = \sum_i y_i m_i b_i = -1.35.3 + 2.28.2 - 1.20.3 = -70 + 112 - 60 = -18 .$$

The smallest positive solution is $z = z' + 140 = 122$.

5.2: Part (a). We have $|(\mathbb{Z}/9)^\times| = \langle [2] \rangle$. So $(\mathbb{Z}/9)^\times \cong C_6 \cong C_2 \times C_3$.

Part (b). We have $(\mathbb{Z}/16)^\times = \langle [3] \rangle \times \langle [15] \rangle \cong C_4 \times C_2$.

Part (c). We have $(\mathbb{Z}/5)^\times - \langle [2] \rangle \cong C_4$.

Part (d). Modulo 25, we have $2^4 \equiv 16 \not\equiv 1$ and $2^{10} \equiv -1 \not\equiv 1$. So $[2]$ does not have order dividing 4 or 10 in the group $(\mathbb{Z}/15)^\times$, which has order 20. By Lagrange's Theorem, $[2]$ must have order 20. Therefore, $(\mathbb{Z}/25)^\times = \langle [2] \rangle \cong C_{20} \cong C_4 \times C_5$.

Part (e). By the Chinese Remainder Theorem,

$$(\mathbb{Z}/30)^\times \cong (\mathbb{Z}/2)^\times \times (\mathbb{Z}/3)^\times \times (\mathbb{Z}/5)^\times \cong C_1 \times C_2 \times C_4 \cong C_2 \times C_4 .$$

5.3: Modulo 9, we have $2^2 \equiv 4 \not\equiv 1$ and $2^3 \equiv 8 \not\equiv 1$. We have $|(\mathbb{Z}/9)^\times| = 6$. So, by Lagrange's Theorem, $[2]_9$ is a generator of $(\mathbb{Z}/9)^\times$.

We shall show that $[2]_{3^n}$ is a generator of $(\mathbb{Z}/3^n)^\times$. We shall argue by induction on n . The case $n = 1$ is clear and the case $n = 2$ is established above. Suppose $n \geq 3$ and that $[2]$ is a generator of $(\mathbb{Z}/3^{n-1})^\times$. Since $[2]_{3^{n-2}}$ is a generator of $(\mathbb{Z}/3^{n-2})^\times$, we have

$$2^{2 \cdot 3^{n-3}} = 1 + 3^{n-2}k$$

for some integer k . Since $[2]_{3^{n-1}}$ is a generator of $(\mathbb{Z}/3^{n-1})^\times$, the integer k is not divisible by 3. Therefore,

$$2^{2 \cdot 3^{n-1}} = (1 + 3^{n-2})^3 \equiv 1 + 3^{n-1}k \not\equiv 1$$

modulo 3^n , as required.

Comment: For any integer $m \geq 1$, an integer a is called a **primitive root** modulo m provided $[a]$ is a generator of $(\mathbb{Z}/m)^\times$. Let p be an odd prime. The above argument generalizes to show that if a is a primitive root modulo p^2 , then a is a primitive root modulo p^n for all $n \geq 2$. This is part of a proof that, for any odd prime p , there exists a primitive root modulo p^n .

5.4: Noting that $(\mathbb{Z}/24)^\times \cong (\mathbb{Z}/3)^\times \times (\mathbb{Z}/8)^\times \cong C_2 \times C_2 \times C_2$, the answer is $n = 24$.

5.5: There are precisely 10 such posets. To find them, consider the Hasse diagram of a toset with size 4, then consider all the ways of extending to a Hasse diagram of a poset with size 5 and height 4. There is 1 extension with no further edges, 6 extensions with 1 further edge, 3 extensions with 2 further edges. (We omit the Hasse diagrams which would take much work to draw using LaTeX.)

Quizzes, with solutions

Laurence Barker, 13 May 2025.

Quiz 1: Consider the cyclic group $C_{10} = \{1, a, a^2, \dots, a^9\}$. Find all the subgroups of C_{10} . Full marks will be awarded for the right answer, without justification.

Solution: The subgroups are $\{1\}$ and $\{1, a^5\}$ and $\{1, a^2, a^4, a^6, a^8\}$ and C_{10} .

Justification: By Lagrange's Theorem, every subgroup of C_{10} has order 1 or 2 or 5 or 10. The subgroups with orders 1 and 10 are plain. Since 2 and 5 are prime, any subgroup with order 2 or 5 must be generated by an element with order 2 or 5, respectively. The only element of C_{10} with order 2 is a^5 . The only elements with order 5 are a^2, a^4, a^6, a^8 , all of which generate the same subgroup.

Comment: The above subgroups are isomorphic to C_1, C_2, C_5, C_{10} . In class, we shall prove that, generally, for any positive integer n , the cyclic group C_n has exactly one subgroup with order d for each divisor d of n , moreover, that group is $\langle a^{n/d} \rangle \cong C_d$.

Quiz 2: Let p and q be primes with q dividing $p - 1$.

(a) Show that there exists an integer a such that $a \not\equiv_p 1$ and $a^q \equiv_p 1$.

(b) Let n be a positive integer. Must there exist an integer a such that $a \not\equiv_{p^n} 1$ and $a^q \equiv_{p^n} 1$?

Solution: Part (a): We have $|(\mathbb{Z}/p)^\times| = p - 1$. By Cauchy's Theorem, the group $(\mathbb{Z}/p)^\times$ has an element $[a]_p$ with order q .

Part (b): We have $|(\mathbb{Z}/p^n)^\times| = p^n - p^{n-1}$, which is divisible by q . Arguing as before, we conclude that the answer is: yes.

Comment 1: Several people found the argument. If you did not get it, that is okay, but you do need to understand the argument now that it has been presented. If you give up on trying to understand the above argument, then you are giving up on the “abstract” bit of “abstract mathematics”.

Comment 2: This is a comment on some more advanced material beyond the scope of the course. Some of you knew or guessed something deeper, along the following lines (which deserves partial credit for a brilliant guess). The following is a standard theorem.

Theorem: *Given a finite field F , then the multiplicative group $F^\times = F - \{0\}$ is cyclic.*

The proof makes use of polynomial rings over fields, together with the fact that a polynomial equation of degree n can have at most n solutions. A generator of the cyclic group $F^\times$ is called a **primitive element** of F . For a prime p , the ring $\mathbb{Z}/p$ is a field. So the group $(\mathbb{Z}/p)^\times$ is cyclic. For example, the elements $[3]$ and $[4]$ are the generators of the group $(\mathbb{Z}/7)^\times \cong C_6$.

If we had covered the above theorem, then we could use it to deduce part (a). But we have not covered it, and it is not on the syllabus. A basic rule for introductory mathematics is that we are not permitted to use a theorem if we do not know a proof of it.

The ring $\mathbb{Z}/p^n$ is not a field when $n \geq 2$. Nevertheless, there is a standard theorem as follows, due to Gauss.

Theorem: (Gauss.) *Given a prime p and a positive integer n , then the group $(\mathbb{Z}/p^n)^\times$ is cyclic except when $p = 2$ and $n \geq 3$, in which case, $(\mathbb{Z}/p^n)^\times$ is isomorphic to the direct product of C_2 and a cyclic group.*

In part (b), $p \neq 2$. So, if we had covered that theorem of Gauss, then we could use it to do part (b).

Quiz 3: Let R be a ring and $\nu \in R$.

(a) Suppose $\nu^2 = 0$. Find the inverse of $1 + \nu$.

(b) Let n be a positive integer and suppose that $\nu^n = 0$. Must $1 + \nu$ have an inverse?

Solution: Part (a). We have $(1 + \nu)^{-1} = 1 - \nu$.

Part (b). Yes, indeed, $(1 + \nu)^{-1} = 1 - \nu + \nu^2 - \dots + (-1)^{n-1}\nu^{n-1}$.

Comment: An example if the situation in part (b) is where $R = \text{Mat}_n(S)$ for any ring S and ν is the matrix in R such that each $(i, i + 1)$ entry is 1 and all the other entries are 0. Putting $n = 4$, we have

$$(1 + \nu)^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Quiz 4: Find all the square roots of -1 in the ring of quaternions $\mathbb{H}$.

Solution: We shall show that the set of square roots of -1 in $\mathbb{H}$ is

$$\{xi + yj + zk : x^2 + y^2 + z^2 = 1\}.$$

Direct calculation shows that every element of that set is a square root of -1 . For the converse, let $q = t + ix + jy + kz$ be such that $q^2 = -1$. By considering the real part, $t^2 - x^2 - y^2 - z^2 = -1$. By the multiplicative property of the norm, $N(q)^2 = N(-1) = 1$. But $N(q)$ is a non-negative real number. So $N(q) = 1$, in other words, $t^2 + x^2 + y^2 + z^2 = 1$. We deduce that $t = 0$ and $x^2 + y^2 + z^2 = 1$.

Comment: Thus, in the 3-dimensional space of pure quaternions $ix + jy + kz$, the points of a sphere with radius 1 and centre 0 are precisely the square roots of -1 .

Quiz 5: Find the isomorphism classes of the connected posets of height 2 and size 5. Draw the Hasse diagrams.

Solution: For any such poset P , every element of P is either maximal or else minimal. The number of such posets with 1, 2, 3, 4 maximal elements is 1, 4, 4, 1, respectively. So there are $1 + 4 + 4 + 1 = 10$ such posets. (I omit the Hasse diagrams, which would take a long time to produce using LaTeX.)

Quiz 6: Which of the following sequences $(x_n)_n$ are rational Cauchy sequences? Just give the answers, no justifications needed.

(a) $x_n = (1/2)^n$.

(b) $x_n = 1$.

(c) $x_n = 2^n$.

Solution: Obviously, (a) and (b) but not (c).

Quiz 7: Working with the usual metric

$$d(x + iy, X + iY) = \sqrt{(x - X)^2 + (y - Y)^2}$$

on $\mathbb{C}$, which of the following subspaces of $\mathbb{C}$ are complete? Just give the answers, no justifications needed.

(a) $\{x + iy \in \mathbb{C} : y > 0\}$.

(b) $\{x + iy \in \mathbb{C} : y \geq 0\}$.

(c) $\mathbb{C}$.

Solution: Not (a), just (b) and (c).

Quiz 8: Let $\mathcal{P}$ be the poset $\{1, 2, 3, 6\}$ partially ordered by division. Find all the nonempty chains in $\mathcal{P}$. How many of them are there?

Solution: Writing $a_1 a_2 \dots$ in place of $\{a_1, a_2, \dots\}$, the chains are:

of length 1: 1, 2, 3, 6,

of length 2: 12, 13, 16, 26, 36,

of length 3: 126, 136,

The total number of nonempty chains is $4 + 5 + 2 = 11$.

Quiz 9: For groups $H \leq G \geq K$, show that $HK \leq G$.

Solution: We must show that the subset $HK \subseteq G$ is closed under inversion and the group operation. Observe that, given $h \in H$, then $hK = Kh$. So, given $k \in K$, then $hk = k'h$ for some $k' \in K$. Since $(hk)^{-1} = k^{-1}h^{-1} = hk'$ for some $k' \in K$, we have closure under inversion. Let $h_1 \in H$ and $k_1 \in K$. Then, for some $k' \in K$, we have $hkh_1k_1 = hh_1k'k_1 \in HK$. We have established closure under the group operation.

Quiz 10: Find all the subgroups of S_3 . Which ones are normal? (Do not forget to include the trivial subgroup and S_3 .)

Solution: The 3 normal subgroups are $\{1\} \cong C_1$ and $\{1, (123), (132)\} \cong C_3$ and S_3 . The other 3 subgroups are $\{1, (12)\}$ and $\{1, (23)\}$ and $\{1, (13)\}$, which are all isomorphic to C_2 .

Quiz 11: Find the conjugacy classes of the group $D_{10} = \langle a, b : a^5 = b^2 = 1, bab^{-1} = a \rangle$.

Solution: We have $ba^i b^{-1} = a^{-i}$ and $a^i b a^{-i} = a^{2i} b$. So the conjugacy classes are

$$\{1\}, \quad \{a, a^4\}, \quad \{a^2, a^3\}, \quad \{b, ab, a^2b, a^3b, a^4b\}.$$

Quiz 12: Find the number of conjugacy classes of S_6 .

Solution: The number of conjugacy classes of S_6 is the number of partitions of 6, which is 11. Indeed, the partitions are

$$6, \quad 5+1, \quad 4+2, \quad 4+1+1, \quad 3+3, \quad 3+2+1, \quad 3+1+1+1, \\ 2+2+2, \quad 2+2+1+1, \quad 2+1+1+1+1, \quad 1+1+1+1+1+1.$$

MATH 124: Abstract Mathematics 2

Midterm 1

17 March 2025, LJB



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.

Remember to justify your answers, except for Question 1, for which no justifications are needed.

1: (20 marks.) Which of the following sequences (x_n) are rational null sequences, and which of them are rational Cauchy sequences? (Just the correct answers will earn full marks. No justifications are needed.)

(a) $x_n = 1/2^n$.

(b) $x_n = 1$ for all n .

(c) $x_1 = 0$ and $x_{n+1} = \sqrt{x_n + 1}$.

(d) $x_n = 3 + \sum_{m=1}^n a_m/2^m$ where $a_m \in \{0, 1\}$ and $\pi = 3 + \sum_{m=1}^{\infty} a_m/2^m$.

(e) $x_n = \sum_{m=1}^n a_m/m!$ where a_m is as in part (d).

2: (20 marks.) Find the smallest positive integer z such that $z \equiv_8 1$ and $z \equiv_3 2$ and $z \equiv_5 3$.

3: (10 marks.) Show that, for any integers a, b, c, n with $c \geq 1$ and $n \geq 2$, there exist infinitely many integers z such that $z \equiv a$ modulo n and $z \equiv b$ modulo $cn + 1$.

4: (30 marks.) Let p and q be distinct odd primes. Which of the following groups are (1) always cyclic, (2) only sometimes cyclic, or (3) never cyclic?

(a) The additive group $\mathbb{Z}/p \times \mathbb{Z}/q$.

(b) The multiplicative group $(\mathbb{Z}/p)^\times \times (\mathbb{Z}/q)^\times$.

5: (20 marks.) Let $\mathcal{R}$ be the ring of rational Cauchy sequences and let I be the ideal of rational null sequences. Let $\mathbb{R}$ denote the copy of the field of real numbers constructed as $\mathbb{R} = \mathcal{R}/I$. Let $\mathbb{Z}_{[2]}$ be the subring of $\mathbb{Q}$ consisting of those rational numbers that have the form $a/2^n$ with $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let $\mathcal{S}$ be the subring of $\mathcal{R}$ consisting of those rational Cauchy sequences whose terms all belong to $\mathbb{Z}_{[2]}$. Show that $\mathbb{R}$ is isomorphic to a quotient ring of $\mathcal{S}$.

Solutions to Midterm 1

1: For sequence (c), $x_2 = \sqrt{2}$ which is irrational, so this is not even a rational sequence. All the others are rational Cauchy sequences. Only (a) is a rational null sequence.

2: Put $n_1 = 8$ and $n_2 = 3$ and $n_3 = 5$. Let $n = n_1 n_2 n_3 = 120$. Write $m_i = n/n_i$. Then $m_1 = 15$ and $m_2 = 40$ and $m_3 = 24$. An inverse of m_1 modulo n_1 is $(-1)^{-1} = -1$. An inverse of m_2 modulo n_2 is $1^{-1} = 1$. An inverse of m_3 modulo n_3 is $(-1)^{-1} = -1$. We have $z \equiv_n z'$ where

$$z' = -1.15.1 + 1.40.2 - 1.24.3 = -15 + 80 - 72 = -7.$$

So $z = 120 - 7 = 113$.

3: Since n and $cn + 1$ are coprime, the existence of z follows from the Chinese Remainder Theorem. Such z is determined only up to congruence modulo $n(cn + 1)$, so there are infinitely many such integers z .

Comment: An alternative proof of the existence of such an integer z is simply to note that we can put

$$z = nc(a - b) + a = (nc + 1)(a - b) + b.$$

4: By the Chinese Remainder Theorem, we have a ring isomorphism $\mathbb{Z}/p \times \mathbb{Z}/q \cong \mathbb{Z}/pq$. Part (a): the above ring isomorphism is also an isomorphism of additive groups, so $\mathbb{Z}/p \times \mathbb{Z}/q$ is always cyclic. Part (b): the multiplicative group $(\mathbb{Z}/p)^\times \times (\mathbb{Z}/q)^\times$ is never cyclic because the distinct elements $(-1, 1)$ and $(1, -1)$ and $(-1, -1)$ all have order 2.

5: We have a ring homomorphism $\theta : \mathcal{S} \rightarrow \mathbb{R}$ given by $\theta(s) = s + I$. We claim that θ is surjective. Let (x_n) be any rational Cauchy sequence. Let a_n be largest integer less than or equal to $2^n x_n$. Then $|a_n/2^n - x_n| \leq 1/2^n$. So the sequences $(a_n/2^n)$ and (x_n) are equivalent. The claim follows. We have $\ker(\theta) = \mathcal{S} \cap I$. So $\mathcal{S}/(\mathcal{S} \cap I) \cong \mathbb{R}$.

MATH 124: Abstract Mathematics 2

Midterm 2

14 April 2025, LJB



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.

Remember to justify your answers.

1: (20 marks) Give one definition of a continuous function $\mathbb{R} \rightarrow \mathbb{R}$. Give an example of a function $f : \mathbb{R} \rightarrow \mathbb{R}$ that is not continuous.

2: (20 marks.) How many isomorphism classes are there of posets that have size 4 and a maximum element? (A maximum element of a poset P is an element m such that $x \leq m$ for all $x \in P$).

3: (20 marks.) The hyperbolic cosine and sine functions are given by the formulas

$$\cosh(x) = \sum_{n=0}^{\infty} x^{2n}/(2n)! , \quad \sinh(x) = \sum_{n=0}^{\infty} x^{2n+1}/(2n+1)! .$$

Give a detailed proof that these infinite summations are convergent for all real x . (Just naming a principle will not be enough.)

4: (20 marks.) Let $f, g : \mathbb{R} \rightarrow \mathbb{R}$ be continuous functions. Show that the composite $f \circ g$ is continuous.

5: (20 marks.) Let p be a prime. Regard $\mathbb{Z}$ as a metric space with distance function d such that, given $x, y \in \mathbb{Z}$ with $x \neq y$, then $d(x, y) = p^{-a}$ where a is the largest natural number for which p^a divides $x - y$. Let $(x_n)_n$ and $(y_n)_n$ be Cauchy sequences in $\mathbb{Z}$ with respect to d .

(a) Show that $(x_n + y_n)_n$ is a Cauchy sequence with respect to d .

(b) Show that $(x_n y_n)_n$ is a Cauchy sequence with respect to d .

Solutions to Midterm 2

1: A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is said to be **continuous** provided, for all $\epsilon > 0$ and all $x \in \mathbb{R}$, there exists a $\delta > 0$ with the property that for any $w \in \mathbb{R}$ satisfying $|w - x| < \delta$, we have $|f(w) - f(x)| < \epsilon$.

An example of a non-continuous function $\mathbb{R} \rightarrow \mathbb{R}$ is f where $f(x) = 0$ for $x < 0$ and $f(x) = 1$ for $x \geq 0$.

Alternative definition: A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is said to be **continuous** provided, for all convergent sequences $(x_n)_n$ in $\mathbb{R}$, we have $f(\lim_n x_n) = \lim_n f(x_n)$.

2: By considering removal of the maximum element, we see that the answer is equal to the number of isomorphism classes of posets with size 3. For the latter, there are 1, 3, 1 with height 1, 2, 3, respectively. So the answer is $1 + 3 + 1 = 5$.

3: This is clear when $x = 0$. So we may assume that $x \neq 0$. Fixing x then, for all sufficiently large n , we have

$$\left| \frac{x^{2(n+1)}/(2(n+1))!}{x^{2n}/(2n)!} \right| < |x^2|/(2n+2) < 1/2.$$

So, by the Ratio Test, the sum for $\cosh(x)$ converges. A similar argument pertains to the sum for $\sinh(x)$.

4: Let $x \in \mathbb{R}$. We must show that $f \circ g$ is continuous at x . Let $\epsilon > 0$. Since f is continuous at $g(x)$, there exists $\eta > 0$ such that, whenever $|g(w) - g(x)| < \eta$, we have $|f(g(w)) - f(g(x))| < \epsilon$. Since g is continuous at x , there exists $\delta > 0$ such that, whenever $|w - x| < \delta$, we have $|g(w) - g(x)| < \eta$.

5: Let $\epsilon > 0$. Choose a such that $p^{-a} < \epsilon$. For all sufficiently large m and n , the integer p^a divides $x_m - x_n$ and $y_m - y_n$.

Part (a). Then p^a divides $x_m + y_m - (x_n + y_n)$.

Part (b). Also, p^a divides $x_m y_m - x_n y_n = x_m(y_m - y_n) + (x_m - x_n)y_n$.

Comment: The metric d in the question is called the **p -adic metric**. It can be extended to $\mathbb{Q}$ in an evident way. In p -adic epsilonics, we tend not to need the $\epsilon/2$ trick.

MATH 124: Abstract Mathematics 2

Final

29 May 2025, LJB



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.

1: (20 marks) **(a)** Define the notion of a uniformly continuous function between metric spaces.

Let X be a metric space with distance function $d : X \times X \rightarrow \mathbb{R}$. Let $z \in X$ and let $f : X \rightarrow \mathbb{R}$ be the function such that $f(x) = d(x, z)$ for $x \in X$.

(b) Must f be continuous? Justify your answer.

(c) Must f be uniformly continuous? Justify your answer.

2: (30 marks.) We shall examine the conjugacy classes of S_6 . Write down a table where:

- The first column lists all the integer partitions $n_1 + n_2 + \dots$ of 6.
- The second column records the size $|[g]_{S_6}|$ of the conjugacy class $[g]_{S_6}$ corresponding to the partition $n_1 + n_2 + \dots$.
- The third column records the size $|C_{S_6}(g)|$ of the centralizer $C_{S_6}(g)$.
- The fourth column says whether or not $C_{S_6}(g)$ is abelian: “yes” if $C_{S_6}(g)$ is abelian, “no” if $C_{S_6}(g)$ is not abelian.

Justify your answers for the row with partition $3 + 3$, but do not justify your answers for the other rows. The first row of the table is as shown.

shape of g	$ [g]_{S_6} $	$ C_{S_6}(g) $	Is $C_{S_6}(g)$ abelian?
$1 + 1 + 1 + 1 + 1 + 1$	1	720	no

Warning: if you present the data in any form that is not an instantly readable single table, then you will not earn full marks.

3: (30 marks.) **(a)** Prove that the symmetric group S_3 has exactly 6 subgroups.

(b) Let p and q be prime numbers and suppose there exists an integer r such that the element $[r]_q$ of $(\mathbb{Z}/q)^\times$ has order p . Show that $q \equiv 1$ modulo p .

(c) For p, q, r as in part (b), let G be the group generated by an element a with order p and an element b with order q such that $aba^{-1} = b^r$. Find the number of subgroups of G .

4: (20 marks.) In this question, if you use the Axiom of Choice, then you must say where you are using it, but you do not need to mention any of the other ZFC axioms. Within the ZFC system, let S be a set. Suppose that, for each $A \in S$, we have

$$A \not\subseteq \bigcup (S - \{A\}).$$

In other words, each element A of S is not contained in the union of all the other elements of S . Show that the unionset $\bigcup S$ has a subset T such that $|T| = |S|$.

Solutions to Final

1: Part (a). For metric spaces X and Y , a function $f : X \rightarrow Y$ is said to be **uniformly continuous** provided, for all $\epsilon > 0$, there exists $\delta > 0$ such that, for all $x, x' \in X$ satisfying $d(x, x') < \delta$, we have $d(f(x), f(x')) < \epsilon$.

Parts (b) and (c) both have answer: yes. Indeed, for all $x, x' \in X$, we have $d(x, z) \leq d(x', z) + d(x, x')$ and $d(x', z) \leq d(x, z) + d(x, x')$. Hence, for any $\epsilon > 0$, if $d(x, x') < \epsilon$, then $d(f(x), f(x')) < \epsilon$.

2: The complete table is as follows.

shape of g	$ [g]_{S_6} $	$ C_{S_6}(g) $	Is $C_{S_6}(g)$ abelian?
1 + 1 + 1 + 1 + 1 + 1	1	720	no
2 + 1 + 1 + 1 + 1	15	48	no
2 + 2 + 1 + 1	45	16	no
2 + 2 + 2	15	48	no
3 + 1 + 1 + 1	40	18	no
3 + 2 + 1	120	6	yes
3 + 3	40	18	no
4 + 1 + 1	90	8	yes
4 + 2	90	8	yes
5 + 1	144	5	yes
6	120	6	yes

For the partition 3+3, to choose an element $g = (a, b, c)(d, e, f)$, there are $6 \cdot 5 \cdot 4 / 3 \cdot 2 = 20$ choices for $\{a, b, c\}$, hence $20/2 = 10$ choices for the partitioning $\{a, b, c\} \cup \{d, e, f\} = \{1, \dots, 6\}$. Then there are 2 choices for the cyclic ordering of a, b, c , also 2 choices for the cyclic ordering of d, e, f . So the associated conjugacy class $[g]$ has size $10 \cdot 2 \cdot 2 = 40$. We have $|C_G(g)| = 720/40 = 18$. The elements (abc) and $(ad)(be)(cf)$ of $C_G(g)$ do not commute, so $C_G(g)$ is non-abelian.

3: Part (a). Let a and b be generators of S_3 such that $a^3 = b^2 = 1$ and $bab^{-1} = a^2$. Then 6 subgroups of S_3 are 1, $\langle a \rangle = \langle a^2 \rangle$, $\langle b \rangle$, $\langle ab \rangle$, $\langle a^2b \rangle$, S_3 . To see that there are no other subgroups, consider a proper subgroup H of G . By Lagrange's Theorem, $|H| = 2$ or $|H| = 3$. So $H = \langle g \rangle$ for some $g \in S_3$. All the possible generators g are already accounted for in the above list of subgroups.

Part (b). By Lagrange's Theorem, the order p of $[r]_q$ divides the order $q - 1$ of the group $(\mathbb{Z}/q)^\times$.

Part (c). The subgroups of G are 1 and G and the proper subgroups. By Lagrange's Theorem, the proper subgroups are the cyclic subgroups with order p or q . Running through all the elements of G , we see that each subgroup with order p has the form $\langle a^k b \rangle$ for some unique $k \in \mathbb{Z}/q$. The only subgroup with order q is the normal subgroup $\langle a \rangle$. So the number of subgroups of G is $q + 3$.

4: For each $A \in S$, let A^* denote the set consisting of those elements of A that do not belong to any other element of S . Then $\{A^* : A \in S\}$ is a set of mutually disjoint nonempty sets. By the Axiom of Choice, there exists a set $T = \{a_A : A \in S\}$ where each $a_A \in A^*$. We have a bijective correspondence $S \leftrightarrow T$ given by $A \leftrightarrow a_A$.