

MATH 3001 ABSTRACT ALGEBRA

Credit Points 10

Legacy Code 200193

Coordinator Roozbeh Hazrat ([https://directory.westernsydney.edu.au/search/name/Roozbeh Hazrat/](https://directory.westernsydney.edu.au/search/name/Roozbeh%20Hazrat/))

Description This subject develops algebraic thought to a high level. The abstract concepts involved in the main topics (group theory and number theory) have many applications in science and technology, and the subject includes an application to cryptography.

School Computer, Data & Math Sciences

Discipline Mathematical Sciences, Not Elsewhere Classified.

Student Contribution Band HECS Band 1 10cp

Check your fees via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 3 subject

Pre-requisite(s) MATH 1006

Equivalent Subjects LGYA 3893 - Advanced Algebra LGYA 3789 - Algebra 3

Learning Outcomes

On successful completion of this subject, students should be able to:

1. recognise, describe and manipulate the basic structures in abstract algebra and number theory; namely, groups, rings and integral domains
2. explain the links between these structures and the symmetries of natural objects
3. apply concepts from group theory and number theory to real life situations, such as RSA cryptography
4. demonstrate proficiency in both spoken and written mathematical communications, particularly constructing and communicating proofs

Subject Content

1. Number Theory - Divisibility, Euclid's algorithm - Prime numbers - Fundamental Theorem of Arithmetic - Theorems of Fermat and Euler - Congruences - Modular arithmetic - Applications to Cryptography: the RSA cryptosystem

2. Ring Theory - Abstract rings and concrete examples - Integral domains and fields - Rings of polynomials - Polynomial congruences and quotients - Fundamental Theorem of Algebra

3. Group Theory - Abstract groups - Subgroups - Direct products - Isomorphism - Permutations, the Symmetric group - Rubik's cube - Cayley's Theorem - Group of units of a ring - Cosets, Lagrange's Theorem, Quotient groups

Number Theory - Divisibility, Euclid's algorithm - Prime numbers - Fundamental Theorem of Arithmetic - Theorems of Fermat and Euler - Congruences - Modular arithmetic - Applications to Cryptography: the RSA cryptosystem

Ring Theory - Abstract rings and concrete examples - Integral domains and fields - Rings of polynomials - Polynomial congruences and quotients - Fundamental Theorem of Algebra

Group Theory - Abstract groups - Subgroups - Direct products - Isomorphism - Permutations, the Symmetric group - Rubik's cube

- Cayley's Theorem - Group of units of a ring - Cosets, Lagrange's Theorem, Quotient groups

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Type	Length	Percent	Threshold	Individual/ Group Task	Mandatory
Intra-session Exam	1 hour	20	N	Individual	Y
Essay	10 hours	20	N	Individual	Y
Presentation	10 minutes	10	N	Individual	Y
Final Exam	Not specified	50	N	Individual	Y

Prescribed Texts

- Nicodemi, Olympia, Sutherland, Melissa A., & Towsley, Gary W. (2007). An introduction to abstract algebra: with notes to the future teacher. Upper Saddle River, N.J.: Pearson Prentice Hall.