THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

This exam paper must not be removed from the venue

Venue ____________________

Seat Number ________

Student Number |__|__|__|__|__|__|__|__|

Family Name ______________________

First Name ______________________

School of Mathematics & Physics

EXAMINATION

Semester One Final Examinations, 2014

MATH3303 Abstract Algebra and Number Theory

This paper is for St Lucia Campus students.

Examination Duration: 120 minutes

Reading Time: 10 minutes

Exam Conditions:

This is a Central Examination

This is a Closed Book Examination - specified materials permitted

During reading time - writing is not permitted at all

This examination paper will be released to the Library

Materials Permitted In The Exam Venue:

(No electronic aids are permitted e.g. laptops, phones)

An unmarked Bilingual dictionary is permitted

Materials To Be Supplied To Students:

none

Instructions To Students:

- This exam is worth 60% of your total assessment.
- You must justify your answers. Solutions given without justification will not receive full marks.
- Each question carries the number of marks shown.
- Answer all questions in the space provided.
- Credit can only be given for work written in this examination script. Use the back of pages & blank pages if required.

For Examiner Use Only

Question	Mark
1	
2	
3	
4	
5	
6	
7	
Total	**100**

Question 1.

(a) Let $\alpha = (3\,4\,1\,2)(2\,4\,5) \in S_5$. Write α as a product of disjoint cycles, and as a product of transpositions. Determine if α is even or odd, and also determine the order of α.

4 Marks

QUESTION 1 CONTINUES ON PAGE 3.

Question 1. [Continued]

(b) List all the conjugacy classes in the group S_4, and determine the size of each class.

5 Marks

QUESTION 1 CONTINUES ON PAGE 4.

Question 1. [Continued]

(c) Using the Class Equation

$$|G| = |Z(G)| + \sum_{x} [G\colon C_G(x)]$$

determine the centre of S_4.

3 Marks

QUESTION 1 CONTINUES ON PAGE 5.

Question 1. [Continued]

(d) Suppose a finite group G acts on a set X. If $x \in X$ then the *orbit* of x is $\{g \cdot x \mid g \in G\}$. The *stabilizer* of x is $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$. It is known that $\mathrm{Stab}(x)$ is a subgroup of G.

Prove that the index of $\mathrm{Stab}(x)$ in G is equal to the size of the orbit of x.

6 Marks

Question 2.

(a) Prove that every group of order 35 is cyclic.

5 Marks

QUESTION 2 CONTINUES ON PAGE 7.

Question 2. [Continued]

(b) Show that there is no simple group of order 30.

5 Marks

QUESTION 2 CONTINUES ON PAGE 8.

Question 2. [Continued]

(c) Prove that a non-abelian group of order 6 is isomorphic to the dihedral group

$$D_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau \rangle.$$

8 Marks

Question 3.

(a) Define a function $\theta\colon \mathbb{Z}[x] \to \mathbb{Z}$ by $\theta(a_0 + \cdots + a_n x^n) = a_0$. Prove that θ is a surjective ring homomorphism.

4 Marks

QUESTION 3 CONTINUES ON PAGE 10.

Question 3. [Continued]

(b) Prove $\ker\theta$ is a prime ideal of $\mathbb{Z}[x]$.

4 Marks

(c) Find a maximal ideal strictly containing $\ker\theta$.

4 Marks

QUESTION 3 CONTINUES ON PAGE 11.

Question 3. [Continued]

(d) Prove that every Euclidean domain is a PID.

Hint: if I is an ideal, pick an element of minimal value with respect to the Euclidean function.

6 Marks

Question 4. Determine if the following rings are fields. Justify your conclusion.

(a) (i) $\mathbb{Q}[x]/\langle x^2+1\rangle$.

(ii) $\mathbb{F}_2[x]/\langle x^2+1\rangle$.

(iii) $\mathbb{Q}[x]/\langle x^4+6x^3+9x+6\rangle$.

3 Marks

QUESTION 4 CONTINUES ON PAGE 13.

Question 4. [Continued]

(b) Show that $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Is it irreducible in $\mathbb{Q}[x]$? Explain.

3 Marks

(c) Construct a field K with 8 elements in which f has a root α.

2 Marks

QUESTION 4 CONTINUES ON PAGE 14.

Question 4. [Continued]

(d) In the field K in (c), express $(1+\alpha)^{-1}$ as a linear combination of non-negative powers of α.

4 Marks

Question 5. Let $R = \{a + b\sqrt{-13} \mid a, b \in \mathbb{Z}\}$. Define a function $N\colon R \to \mathbb{Z}$ by $N(z) = |z|^2$. You may assume that R is an integral domain and that $N(wz) = N(w)N(z)$ for all w, $z \in R$.

(a) Show that $N(a + b\sqrt{-13}) = a^2 + 13b^2$. Deduce that $R^\times = \{\pm 1\}$.

3 Marks

(b) Show that there is no element $r \in R$ with $N(r) = 2$ or $N(r) = 7$.

2 Marks

QUESTION 5 CONTINUES ON PAGE 16.

Question 5. [Continued]

(c) By considering the factorization below (or otherwise), show that R is not a UFD.

$$14 = 2 \cdot 7 = (1 + \sqrt{-13}\,)(1 - \sqrt{-13}\,)$$

5 Marks

Question 6.

(a) (i) Let $n \geq 2$ and let F_n be the Fermat number $F_n = 2^{2^n} + 1$. Show that if p is a prime factor of F_n then $p = 2^{n+1}k + 1$ for some integer k.

Hint: Consider the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.

4 Marks

(ii) Prove that the integer k in (i) must be even.
Hint: is 2 a quadratic residue mod p?

4 Marks

QUESTION 6 CONTINUES ON PAGE 18.

Question 6. [Continued]

(b) Suppose q is prime and $p = 2q + 1$ is also prime. If $\left(\frac{a}{p}\right) = -1$ and $a \not\equiv -1 \pmod{p}$, show that a is a primitive root mod p (that is, show that a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$).

Hint: Euler's Criterion.

6 Marks

Question 7. Let R be a ring with identity. Using Zorn's Lemma, prove that R has a maximal ideal.

10 Marks

[This page intentionally left blank for your working.]