2009 A SEMESTER EXAMINATIONS

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

DEPARTMENT	Mathematics
PAPER TITLE	Algebra and Number Theory
TIME ALLOWED	Three hours
NUMBER OF QUESTIONS IN EXAMINATION PAPER	Twelve
NUMBER OF QUESTIONS TO BE ANSWERED	Ten
VALUE OF EACH QUESTION	10 marks
GENERAL INSTRUCTIONS	Answer FIVE questions from SECTION A and FIVE questions from SECTION B. Total marks available: 100.
SPECIAL INSTRUCTIONS	Polyhedral models are permitted.
CALCULATORS PERMITTED	No.

SECTION A

(Answer FIVE of the SIX questions.)

1. Unless requested otherwise, permutations should be written as products of disjoint cycles. Consider the following elements of S_7.

$$\alpha = (13)(4567) \qquad \beta = (1234)(67) \qquad \gamma = (1357)(246)$$

(a) Compute $\alpha\beta$.

(b) Compute $\beta\alpha$.

(c) Compute γ^{-1}.

(d) Compute the conjugate γ^{α}.

(e) Compute γ^{20}.

(f) Write α as a product of 2-cycles.

(g) List the elements of $\{\alpha.\beta, \gamma\} \cap A_7$.

(h) Compute the orders $|\alpha|$, $|\beta|$ and $|\gamma|$.

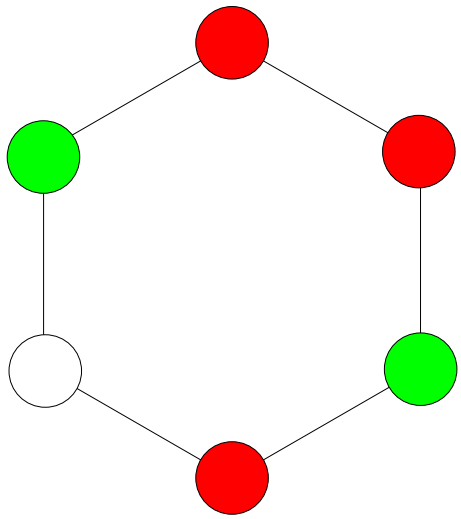
(i) List the elements of the cyclic subgroup $< \beta >$.

(j) Two of the given permutations are conjugate. Find a permutation π that conjugates one onto the other. Check your answer by direct calculation.

2.

(a) State Burnside's counting theorem.

(b) You are making bracelets by putting six coloured beads on a loop of string. There are three colours available. How many distinct necklaces can you make?



3. (a) List the elements of the group $\mathbb{Z}_{30}^*$ of units in the integers modulo 30 under multiplication.

(b) State the Fundamental Theorem of Abelian Groups and explain what it tells us about the group $\mathbb{Z}_{30}^*$.

(c) Identify (fully stating your reasons) which of the possibilities you identified as being isomorphic to $\mathbb{Z}_{30}^*$ is correct.

4. (a) For any group G, define what it means for a subgroup $N \leq G$ to be normal.

(b) If G is a group with $H \leq G$ and $N \trianglelefteq G$, define HN and show that it is a subgroup.

(c) Let K and N be two normal subgroups of a group G with $K \leq N$, and let $H \leq G$ be any subgroup. Prove that $(KH) \cap N = K(H \cap N)$.

5. (a) State Lagrange's Theorem for finite groups.

(b) Let G be a finite group. Prove that if $|G|$ is prime, then G is cyclic.

(c) Let G be a finite group, with $H \leq G$. Prove that the normaliser $N_G(H)$ is a subgroup of G, where

$$N_G(H) = \{g \in G : g^{-1}hg \in H \ \forall\, h \in H\}.$$

6. (a) Let G be a group with $N \trianglelefteq G$.

i. Define the quotient group G/N. You need not prove it is a group.

ii. Define the natural projection $\pi : G \longrightarrow G/N$ and prove it is a homomorphism.

(b) State the Fundamental Theorem of Homomorphisms for groups.

(c) Let $H \trianglelefteq G$ and $K \trianglelefteq G$. Prove that $G/(H \cap K)$ is isomorphic to a subgroup of $G/H \times G/K$.

SECTION B

(Answer FIVE of the SIX questions.)

7. (a) i. State the subring test.

ii. Hence prove that the set of S of 2×2 matrices with real entries

$$S = \{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \}$$

is a subring of $M_2(\mathbb{R})$.

(b) i. When is a ring R said to be an *integral domain*?

ii. Give the multiplication table for $\mathbb{Z}_4$. Is it an integral domain? Why/why not?

8. (a) State the Division Algorithm for polynomials over a field $\mathbb{F}$.

(b) Hence prove the Remainder Theorem: for $a \in \mathbb{F}$ and $p(x) \in \mathbb{F}[x]$, the remainder of $p(x)$ on division by $(x - a)$ is $p(a)$.

(c) Hence compute the remainder of $x^{10} + 3x^5 + 2x^3 + 4x^2 + x + 1 \in \mathbb{Z}_7$ on division by $x - 1$.

(d) *Giving reasons*, decide whether the polynomial $p(x) = 3x^3 + 4 \in \mathbb{Z}_5[x]$ is irreducible.

9. (a) Define what it means for I to be an ideal of the ring R.

(b) If I is an ideal of a ring R with identity 1, show that $I = R$ if $1 \in I$.

(c) Hence show that a field has no proper non-trivial ideals (that is, its only ideals are itself and $\{0\}$).

(d) Let R be a commutative ring with identity.

i. When is an ideal I of R said to be *prime*?

ii. Show that if $I \triangleleft R$ is prime then R/I has no zero divisors.

(e) Give an example of an ideal of a commutative ring with identity which is prime but not maximal (no proof needed).

10. Let $\mathbb{R}$ and $\mathbb{C}$ be the real and complex number fields respectively, and define

$$f : \mathbb{R}[x] \to \mathbb{C}$$

by setting $f(p(x)) = p(i) \in \mathbb{C}$ for all $p(x) \in \mathbb{R}[x]$ (that is, temporarily view $p(x) \in \mathbb{R}[x]$ as a polynomial in $\mathbb{C}[x]$ and evaluate $p(i)$).

(a) Show that f is a surjective homomorphism.

(b) Hence deduce the existence of a factor ring of the form $\mathbb{R}[x]/ < p(x) >$ which is isomorphic to $\mathbb{C}$.

(c) Explicitly give a suitable $p(x) \in \mathbb{R}[x]$ for Part (b) above, and explain your choice.

(d) Why is $< p(x) >$ maximal?

11. Recall that an integral domain D is said to be a Euclidean domain if there is a valuation function $d : D\backslash\{0\} \to \{0, 1, 2, \ldots\}$, satisfying

$$\text{if } a, b \in D \text{ with } b \neq 0, \text{ there are } q, r \in D \text{ such that}$$

$$a = bq + r \text{ with } r = 0 \text{ or } d(r) < d(b).$$

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

(b) Recall $\mathbb{Z}[i]$ is a Euclidean domain if we define $d(a + bi) = a^2 + b^2$ for all $a, b \in \mathbb{Z}$ (not both zero).
Find $q, r \in \mathbb{Z}[i]$ such that $2 - 3i = 2iq + r$, where $r = 0$ or $d(r) < d(2i)$.

12. (a) In the quaternions $\mathbb{H}$, find the inverse of $a = 2 - 2\mathbf{i} - \mathbf{j} + \mathbf{k}$, and hence solve the quaternionic equation $ax = 20\mathbf{i}$ for the unknown quaternion x, expressing your answer in standard form $x = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$.

(b) On any ring R, we can define the operation $a \circ b = a + b + ab$.

i. Show that $\circ$ is associative.

ii. Show that the modified distributive law given by

$$a \circ (b + c) = (a \circ b) + (a \circ c) - a$$

holds for all $a, b, c \in R$.
(There is a similar law involving $(a + b) \circ c$, but do not bother to show this!)