Math 222 Final Exam: Thursday, May 8, 1997; 1:45–3:45pm

Instructions. This exam contains six questions, all of equal value. Calculators may be used if desired. Throughout the exam, $\mathbf{Z}$ denotes the integers, $\mathbf{Q}$ denotes the rational numbers, $\mathbf{C}$ denotes the complex numbers, $\mathbf{H}$ denotes the ring of quaternions and $\mathbf{Z}_m$ denotes the integers modulo m.

1. *(25 points)*

(a) Describe all the integers x satisfying the congruence $6x \equiv 7 \pmod{19}$.

(b) Evaluate $(2 - 3i + 4j - k)^{-1}$ in $\mathbf{H}$.

(c) Find all complex numbers z with $z^3 = -1$.

(d) Calculate $(2 + 3\sqrt{3})^{-1}$ in $\mathbf{Q}[\sqrt{3}]$.

(e) Write down the prime factorizations of all positive integers dividing $7^2 \cdot 23$, and the factorizations into irreducible polynomials of all the polynomials in $\mathbf{Z}_2[t]$ which divide $(t+1)^2(t^2+t+1)$.

2. *(25 points)*

(a) Let F be a field, and $h \in F[t]$ be a polynomial. Explain what is meant by saying that h is irreducible. Under what assumptions on h will the quotient ring $F[t]/\langle h \rangle$ be a field (here, $\langle h \rangle$ denotes the principal ideal of $F[t]$ generated by h).

(b) In the polynomial ring $\mathbf{Z}_2[t]$, express the greatest common divisor $d = 1$ of the polynomials $f = t^2 + t + 1$ and $g = t^3 + t + 1$ in the form $d = af + bg$ for suitable $a, b \in R$.

(c) Show that in the quotient ring $R = \mathbf{Z}_2[t]/\langle g \rangle$, one has $\overline{f}^{\,-1} = \overline{a}$ and hence calculate the inverse of $\overline{f}$ explicitly.

(d) Is g irreducible? Is R a field? Justify your answers.

3. *(25 points)* Consider the following subsets A, B, I of the complex numbers.

(i) $A = \{a + bi \mid a, b \in \mathbf{Z}\}$.
(ii) $B = \{a + bi \mid a, b \in \mathbf{Q}\}$.
(iii) $I = \{a + bi \mid a, b \text{ both even integers}\}$.

(a) Explain why A and B are subrings of $\mathbf{C}$.

(b) Show that I is equal to the principal ideal of A generated by 2.

(c) Show that in the quotient ring A/I, one has $\overline{a + bi} = \overline{a' + b'i}$ where a' and b' are the remainders on division of the integers a and b by 2 (e.g. $\overline{2 + 3i} = \overline{i}$). Conclude that A/I has only four elements, namely $A/I = \{\overline{0}, \overline{1}, \overline{i}, \overline{1 + i}\}$.

(d) Write down the multiplication and addition tables for A/I. Is A/I a field or an integral domain?

(e) Show I is not an ideal of B. Is either A or B a field? Is I a subring of $\mathbf{C}$? Justify your answers.

4. *(25 points)*

(a) Decide which of the following subsets A, B, C of the plane $\mathbf{R} \times \mathbf{R}$ form a group under the operation $(x, y) + (x', y') = (x + x', y + y')$. Explain your reasons.

(i) $A = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x \geq 0\}$
(ii) $B = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x + y = 0\}$
(iii) $C = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x + y = 1\}$.

(b) Let Q denote the subgroup $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ of the unit group $\mathbf{H}^*$ of the quaternions. Show that $N = \{\pm 1, \pm j\}$ is a normal subgroup of Q. List explicitly all the left cosets gN, for $g \in Q$, of N in Q and write down the multiplication table for the quotient group Q/N.

5. *(25 points)* In this question, S_n denotes the symmetric group on n letters.

(a) In S_5, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$. Calculate τ^{-1} and $\tau\sigma\tau^{-1}$.

(b) For $1 \leq i \leq j \leq n$, let (i, j) denote the 2-cycle in S_n which swaps i and j and maps k to itself if k is different from i and j. Calculate the product $(1,5)(1,4)(1,3)(1,2)$ in S_5 and determine its order.

(c) List the 6 elements of the symmetric group S_3 explicitly. Let A be the subgroup of S_3 consisting of the identity permutation and the 2-cycle $(1, 2)$. Explicitly find all the left cosets gA, for $g \in S_3$, of A in S_3.

(d) Define the order $|G|$ of a group G and the index $[G\colon H]$ of a subgroup H of G. What is the relation between $|H|$, $|G|$ and $[G\colon H]$?

(e) Does S_3 have any subgroup with 4 elements? Justify your answer.

6. *(25 points)* In this question, $\mathbf{C}^*$ denotes the group of non-zero complex numbers under multiplication, and $\mathbf{R}$ denotes the group of real numbers under addition.

(a) Write down the rule for multiplication of complex numbers in polar form. Hence show that the function $\phi\colon \mathbf{R} \to \mathbf{C}^*$ given by $\phi(x) = \cos 2\pi x + i \sin 2\pi x$ is a group homomorphism

(b) Check that the image $Im\ \phi$ is the "circle group" $\mathbf{S}^1$ consisting of the "unit circle" of complex numbers of absolute value 1.

(c) Show that the kernel $ker\ \phi$ is the group $\mathbf{Z}$ of integers under addition.

(d) State the fundamental homomorphism theorem for a homomorphism $\theta\colon G \to H$ of groups.

(e) Conclude using (d) that there is an isomorphism of groups $\mathbf{R}/\mathbf{Z} \cong \mathbf{S}^1$.