FALL 2005 PRELIMINARY EXAMINATION SOLUTIONS

1A. Let M be a compact metric space and let $(U_i)_{i\in I}$ be an open cover of M. Show that there exists $\varepsilon > 0$ such that, for all $x, y \in M$, if $d(x, y) < \varepsilon$ then there is some j with both x and y in U_j.

Solution: Suppose not. Then for each positive integer n there are points $x_n, y_n \in M$ with $d(x_n, y_n) < 1/n$, and there is no $j \in I$ with $x_n, y_n \in U_j$. Since M is compact, there is a subsequence of the x_n's converging to some point $p \in M$. Of course there is some U_j with $p \in U_j$. The corresponding subsequence of the y_n's also converges to p. Hence there is some sufficiently large N with both x_N and $y_N \in U_j$, because U_j is an open neighborhood of p. This is a contradiction.

2A. Prove that, if $f(z) = P(z)/Q(z)$ is a rational function with complex coefficients whose numerator has lower degree than the denominator, then $f(z)$ is a sum of terms of the form $a/(z-b)^k$, with $a, b \in \mathbb{C}$.

Solution: We may assume that Q is monic. Let $Q(z) = \prod_{i=1}^{k}(z-r_i)^{n_i}$ be the factorization of Q into powers of distinct linear factors. We will try to write

$$\frac{P(z)}{Q(z)} = \sum_{i=1}^{k}\sum_{j_i=1}^{n_i}\frac{a_{ij_i}}{(z-r_i)^{j_i}}, \tag{1}$$

where the a's are constants to be chosen. The number of such constants equals the degree n of Q.

The right hand side of (1) is a rational function whose denominator is Q and whose numerator is a polynomial of degree (at most) $n-1$. The space of such polynomials has dimension n over $\mathbb{C}$, so we have a linear map from the a's to this numerator which maps between n-dimensional vector spaces. Our goal is to show that it is onto; it suffices to show that it is one-to-one, i.e. that its kernel is zero, i.e. that the right hand side of (1) is zero only if all the a's are zero.

To prove the last statement above, we consider the limiting behavior of the right hand side as z approaches one of the r_i's. All the terms except those with $z - r_i$ in the denominator have finite limits, while the sum of the remaining terms goes to infinity like $1/(z-r_i)^p$, where p is the largest index, if any, for which a_{ip} is not equal to zero. If the entire sum is to be zero, the limit must be zero, hence finite, and so all the a's must vanish.

3A. Define $U \subseteq \mathbb{C}$ to be the open right half plane with the interval $(0, 1] \subseteq \mathbb{R}$ deleted. Find an explicit conformal equivalence of U with the open unit disk D.

Solution: If a map is a holomorphic bijection from one open set to another, it is a conformal equivalence.

(1) Let $T_1(z) = z^2$. Then T_1 maps U conformally onto $\mathbb{C}\backslash L$, where $L = \{x \in \mathbb{R} : x \le 1\}$.

(2) Next, let $T_2(w) = w - 1$, so that $T_2T_1(U) = \mathbb{C}\backslash\{x \in \mathbb{R} : x \le 0\}$.

(3) Let $T_3(z) = z^{1/2}$, the principal branch — so $T_3T_2T_1U = P$, the open right half plane.

(4) The fractional linear map $T_4(z) = \dfrac{z-1}{z+1}$ is a conformal equivalence of P with D . Hence $S = T_4T_3T_2T_1$ is a conformal equivalence of U with D.

4A. Let m and n be positive integers. Prove that the ideal generated by $x^m - 1$ and $x^n - 1$ in $\mathbb{Z}[x]$ is principal.

Solution: Let $d = \gcd(m, n)$. We claim that $(x^d - 1) = (x^m - 1, x^n - 1)$ as ideals of $\mathbb{Z}[x]$. First,

$$x^m - 1 = (x^d - 1)(x^{m-d} + x^{m-2d} + \cdots + x^d + 1)$$

so $x^d - 1$ divides $x^m - 1$. Similarly $x^d - 1$ divides $x^n - 1$. Thus $(x^m - 1, x^n - 1) \subseteq (x^d - 1)$.

On the other hand, the image of x in the ring $\mathbb{Z}[x]/(x^m-1, x^n-1)$ is a unit of multiplicative order dividing m and dividing n, so its order divides d. In other words, $x^d \equiv 1 \pmod{x^m - 1, x^n - 1}$, so $(x^d - 1) \subseteq (x^m - 1, x^n - 1)$. Thus $(x^d - 1) = (x^m - 1, x^n - 1)$.

Alternative approach to the last paragraph: Using the identity

$$x^n - 1 = x^{n-m}(x^m - 1) + (x^{n-m} - 1),$$

one could show that for $n \geq m$, we have $(x^m - 1, x^n - 1) = (x^m - 1, x^{n-m} - 1)$, and then one could use the Euclidean algorithm on the exponents, to prove that $x^d - 1 \in (x^m - 1, x^n - 1)$.

5A. Is there a differentiable function $f\colon \mathbb{R} \to \mathbb{R}$ satisfying $f(0) = 1$ and $f'(x) \geq f(x)^2$ for all $x \in \mathbb{R}$?

Solution: We will show that no such function f exists. Suppose f satisfies the conditions. First, $f(x) > 0$ on $[0, \infty)$, because $f(0) = 1$ and $f'(x) \geq f(x)^2 \geq 0$. For $x \geq 0$, integrating $f'(x)/f(x)^2 \geq 1$ from 0 to x yields $1 - 1/f(x) \geq x$. It follows that $f(x) \geq 1/(1 - x)$ on $[0, 1)$, so $\lim_{x\to 1} f(x)$ does not exist, contradicting the continuity of f.

6A. Let A be an $n \times n$ matrix with real entries such that $(A - I)^m = 0$ for some $m \geq 1$. Prove that there exists an $n \times n$ matrix B with real entries such that $B^2 = A$.

Solution: Write $A = I + N$, so $N^m = 0$. Let $P(x)$ be the m-th Taylor polynomial of the function $\sqrt{1 + x}$, so $P(x)^2 \equiv 1 + x \pmod{x^m}$. In other words

$$P(x)^2 = 1 + x + x^m Q(x)$$

for some $Q(x) \in \mathbb{R}[x]$. Then

$$P(N)^2 = I + N + N^m Q(N) = I + N = A,$$

so $B := P(N)$ satisfies $B^2 = A$.

Alternative solution: The minimal polynomial of A divides $(x - 1)^m$, so all eigenvalues of A are 1. Since the eigenvalues are real, A can conjugated over $\mathbb{R}$ into Jordan canonical form.

It suffices to prove the result for each Jordan block. Thus we may assume that

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1. \end{pmatrix}$$

It suffices to find one matrix A' conjugate over $\mathbb{R}$ to A such that A' is a square.

We claim that $A' := A^2$ has this property. Of course it is a square. Since A' is upper triangular with 1s along the main diagonal, its eigenvalues are all 1. If A is $n \times n$, then $A' - I$ has rank $n-1$, since $A' - I$ is strictly upper triangular and deleting its first column and last row results in an invertible matrix (with 2s on the diagonal). Thus A' has the same Jordan canonical form as A, so it is conjugate to A over $\mathbb{R}$.

7A. Let $f(z) = z^5 + 5z^3 + z^2 + z + 1$. How many zeros (counting multiplicity) does f have in the annulus $1 \leq |z| \leq 2$?

Solution: The polynomial f has no zeros in the annulus. We use Rouché's theorem. Let $g(z) = 5z^3$. Then on the circle $|z| = 2$,

$$|f(z) - g(z)| = |z^5 + z^2 + z + 1| \leq 32 + 4 + 2 + 1 = 39.$$

But $|g(z)| = 40$. So $|f(z) - g(z)| < |g(z)|$ on this circle. Therefore f has 3 zeros inside the circle $|z| = 2$.

Now consider $|z| = 1$. We get

$$|f(z) - g(z)| = |z^5 + z^2 + z + 1| \leq 4$$

while $|g(z)| = 5$. Accordingly f has 3 zeros inside the circle $|z| = 1$.

Thus f has no zeros with $1 \leq |z| \leq 2$.

8A. Find the smallest n for which the permutation group S_n contains a cyclic subgroup of order 111.

Solution: Let the partition $n = n_1 + n_2 + ... + n_k$ represent the cycle structure of an element $g \in S_n$, *i.e.* g is a products of commuting cycles of the lengths $n_1 \leq n_2 \leq ... \leq n_k$. The order of the cyclic subgroup generated by g is obviously equal to the least common multiple of $n_1, ..., n_k$. We want this least common multiple to be $111 = 3 \cdot 37$. One of the possibilities is $(n_1, n_2, ..., n_k) = (3, 37)$ in which case $n = 3 + 37 = 40$. We claim that this value of n is the minimal possible. Indeed, if 111 is the least common multiple of $n_1, ..., n_k$ then each of the prime factors $3, 37$ divides at least one of the numbers n_i and moreover, the sum of such factors dividing n_i does not exceed their product and thus does not exceed n_i. This implies $n = n_1 + ... + n_k \geq 3 + 37 = 40$.

9A. A doubly infinite sequence $(a_j)_{j \in \mathbb{Z}}$ of real numbers is said to be **rapidly decreasing** if, for each positive integer n, the sequence $j^n a_j$ is bounded. Let (a_j) and (b_j) be rapidly decreasing sequences, and define the convolution of these sequences by $c_j = \sum_{k \in \mathbb{Z}} a_k b_{j-k}$ for $j \in \mathbb{Z}$. Prove that the series defining each c_j is convergent, and that (c_j) is a rapidly decreasing sequence.

Solution: For any $n \geq 0$, the boundedness of $j^{n+2}a_j$ implies that the series $\sum_{j \neq 0} |j^n a_j|$ is dominated by a constant times $\sum_{j \neq 0} 1/j^2$, so $\sum_{j \in \mathbb{Z}} |j^n a_j|$ converges. Similarly $\sum_{j \in \mathbb{Z}} |j^n b_j|$ converges.

The series defining c_j converges absolutely, since

$$\sum_{k \in \mathbb{Z}} |a_k||b_{j-k}| \leq \left(\sum_{k \in \mathbb{Z}} |a_k| \right) \left(\sum_{\ell \in \mathbb{Z}} |b_\ell| \right).$$

To show that (c_j) is rapidly decreasing, it suffices to prove that $\sum_{j \in \mathbb{Z}} |j^n c_j|$ converges for each $n \geq 1$. In fact,

$$\begin{aligned}
\sum_{n \in \mathbb{Z}} |j^n c_j| &\leq \sum_{k \in \mathbb{Z}} \sum_{\ell \in \mathbb{Z}} |(k+\ell)^n a_k b_\ell| \\
&= \sum_{k \in \mathbb{Z}} \sum_{\ell \in \mathbb{Z}} \sum_{i=0}^{n} \binom{n}{i} k^i \ell^{n-i} |a_k||b_\ell| \\
&= \sum_{i=0}^{n} \binom{n}{i} \left(\sum_{k \in \mathbb{Z}} |k^i a_k| \right) \left(\sum_{\ell \in \mathbb{Z}} |\ell^{n-i} b_\ell| \right),
\end{aligned}$$

and each infinite sum in the last expression converges.

1B. How many pairs of integers (a, b) are there satisfying $a \geq b \geq 0$ and $a^2 + b^2 = 5 \cdot 17 \cdot 37$?

Solution: Representations of n as $a^2 + b^2$ are in bijection with factorizations of the form $n = (a + bi)(a - bi)$. Multiplying $a + bi$ by a unit (power of i) and replacing it by its complex conjugate corresponds to replacing (a, b) by one of $(\pm a, \pm b)$ or $(\pm b, \pm a)$. Also, no representations of $5 \cdot 17 \cdot 37$ have $a = b$ or $b = 0$, since $5 \cdot 17 \cdot 37$ is odd and not a square.

Thus the problem is reduced to finding the number of factorizations of $5 \cdot 17 \cdot 37$ as $\alpha\bar{\alpha}$, where α is considered up to conjugation and multiplication by units. In the PID $\mathbb{Z}[i]$, we have

$$5 \cdot 17 \cdot 37 = (2+i)(2-i)(4+i)(4-i)(6+i)(6-i).$$

In order to have $\alpha\bar{\alpha} = 5 \cdot 17 \cdot 37$, the number α must be divisible by exactly one of $2+i$ and $2-i$, exactly one of $4+i$ and $4-i$, and exactly one of $6+i$ and $6-i$. And conversely, choosing one factor from each pair determines α up to a unit. This gives 8 values of α, and they form 4 complex conjugate pairs, so the answer to the problem is 4.

2B. Let f be a continuous real-valued function defined on $[0, \infty)$, each that $f(x) \geq 0$, f is non-increasing, and $\lim_{x \to \infty} f(x) = 0$. Show that

$$\lim_{R \to \infty} \int_0^R f(x) \sin x \; dx$$

exists. (In other words, the improper integral

$$\int_0^\infty f(x) \sin x \; dx$$

converges.)

Solution: For each integer $n \geq 0$, let

$$\begin{aligned} a_n &= \int_{n\pi}^{(n+1)\pi} f(x)|\sin x|\ dx \\ &= \int_0^{\pi} f(x+n\pi)|\sin x|\ dx. \end{aligned}$$

Then for all n, $a_n \geq 0$ and $a_n \geq a_{n+1}$ because the function f is non-increasing. Moreover $a_n \to 0$ as $n \to \infty$ because $f(x+n\pi) \to 0$ as $n \to \infty$, uniformly on $[0, \pi]$.)

Moreover

$$\begin{aligned} \int_0^{(n+1)\pi} f(x) \sin x\ dx &= \sum_{k=0}^{n} \int_{k\pi}^{(k+1)\pi} f(x) \sin x\ dx \\ &= a_0 - a_1 + a_2 \pm \cdots + (-1)^n a_n. \end{aligned}$$

From the alternating series theorem,

$$\lim_{n\to\infty} \int_0^{(n+1)\pi} f(x) \sin x\ dx$$

exists. This clearly implies that

$$\lim_{R\to\infty} \int_0^{R} f(x) \sin x\ dx$$

exists.

3B. For which pairs of monic polynomials $(p(x), m(x))$ over the complex numbers does there exist a matrix in $M_{n,n}(\mathbb{C})$ whose characteristic polynomial is $p(x)$ and whose minimal polynomial is $m(x)$?

Solution: By the Cayley-Hamilton theorem, if p and m are the characteristic and minimal polynomials of a matrix A, then p is divisible by m. There is another condition: every root of p is a root of m. To see this, let r be a root of p, i.e. an eigenvalue of A, and let v be a corresponding eigenvector. Then $0 = m(A)$, so $0 = m(A)v = m(r)v$. Since $v \neq 0$, we must have $m(r) = 0$.

Now we will show that these two necessary conditions are sufficient. We may write p as a product $\prod_{j=1}^{d}(x - r_j)^{n_j}$, where each multiplicity n_j is a positive integer. Then m must have the form $\prod_{j=1}^{d}(x - r_j)^{m_j}$, where $1 \leq m_j \leq n_j$. Now we construct A in block diagonal form, with d blocks, where the j'th block is itself block diagonal consisting of 2 blocks. The first is an $m_j \times m_j$ elementary Jordan block with r_j on the diagonal, and the other (which might be reduced to nothing) is simply r_j times the identity.

4B. Determine which numbers $a \in \mathbb{C}$ have the following property: There exists an analytic function f defined in the open unit disk such that, for all integers $n \geq 2$,

$$f(1/n) = 1/(n+a).$$

Solution: Obviously $f(0) = 0$. Also, for $z_n = 1/n$,

$$f(z_n) = z_n/(1 + az_n).$$

Since 0 is an accumulation point of the z_n's, we must have

$$f(z) = z/(1 + az)$$

in some neighborhood of 0. But the latter function is analytic in the open disk $|z| < 1$ if and only if $|a| \leq 1$.

5B. Given a prime number p, let $\mathbb{F}_p$ be the field of p elements, and let R be the ring $\mathbb{F}_p[x]/(x^3)$. For which primes p is the unit group R^* cyclic?

Solution: We will show that R^* is cyclic if and only if $p = 2$. Let $\bar{x}$ be the image of x in R.

First suppose $p \geq 3$. Since R has characteristic p, the p-th power map $R \to R$ is a ring homomorphism, and

$$(1 + a\bar{x} + b\bar{x}^2)^p = 1^p + a^p\bar{x}^p + b^p\bar{x}^{2p} = 1 + a^p \cdot 0 + b^p \cdot 0 = 1$$

for any $a, b \in \mathbb{F}_p$. Thus R^* contains at least p^2 elements of order dividing p. But a cyclic group contains at most p elements of order dividing p, so R^* cannot be cyclic.

Now suppose $p = 2$. We calculate that $(1 + \bar{x})^4 = 0$ but $(1 + \bar{x})^2 \neq 0$, so $1 + \bar{x}$ generates a cyclic group of order 4 in R^*. On the other hand, of the 8 elements of R, the 4 elements of the form $a\bar{x} + b\bar{x}^2$ with $a, b \in \mathbb{F}_2$ form a proper ideal of R, so these elements are not units, so R^* has at most $8 - 4 = 4$ elements. Thus R^* is cyclic of order 4, generated by $1 + \bar{x}$.

6B. Let $K \subset \mathbb{R}^n$ be closed, convex, and nonempty. (*Convex* means that if $x, y \in K$ and $\lambda \in [0, 1]$ then $\lambda x + (1 - \lambda)y \in K$.) Show that for every $x \in \mathbb{R}^n$, there exists $y \in K$ that uniquely minimizes the Euclidean distance to x, i.e. $\|x - y\| < \|x - z\|$ for all $z \in K \setminus \{y\}$.

Solution: Let B be a closed ball of radius r centered at x. Since K is nonempty, we can choose r sufficiently large so that $K \cap B \neq \emptyset$. Since $K \cap B$ is compact, the continuous function $f(y) = \|x - y\|$ on $K \cap B$ takes a minimum d at some $y \in K \cap B$. Then $\|x - z\| \geq d$ for all $z \in K$, since if $z \in K \setminus B$ then $\|x - z\| > r \geq d$.

To prove uniqueness of the distance minimizer y, suppose $z \in K$ is a different point satisfying $\|x - z\| = d$. By convexity, $w = (y + z)/2 \in K$. Then $\|x - w\|$ is the height of an isosceles triangle with equal sides of length d, so $\|x - w\| < d$, contradicting the minimality.

7B. Let V be a finite-dimensional complex vector space equipped with a positive-definite Hermitian inner product. Let $T\colon V \to V$ be a Hermitian (i.e., self-adjoint) linear operator. Prove that

(a) $1 + iT$ is nonsingular (where $i = \sqrt{-1}$); and
(b) $(1 - iT)(1 + iT)^{-1}$ is a unitary operator.

Solution:

(a) If not, let v be a nonzero vector such that $(1 + iT)v = 0$. Then $Tv = iv$, contradicting the fact that eigenvalues of a Hermitian operator are real.

(b) Let $A = (1 - iT)(1 + iT)^{-1}$. Then

$$A^* = ((1+iT)^{-1})^*(1-iT)^* = ((1+iT)^*)^{-1}(1-iT)^* = (1-iT^*)^{-1}(1+iT^*) = (1-iT)^{-1}(1+iT),$$

since T is Hermitian. Thus

$$A^*A = (1 - iT)^{-1}(1 + iT)(1 - iT)(1 + iT)^{-1}.$$

But $1 + iT$ and $1 - iT$ commute (their product in either order is $1 + T^2$), so

$$A^*A = (1 - iT)^{-1}(1 - iT)(1 + iT)(1 + iT)^{-1} = I \cdot I = I.$$

Thus A is unitary.

Alternative solution: If we choose an orthonormal basis of eigenvectors of T as basis, then the matrix of T is diagonal, with real numbers $\lambda_1, \ldots, \lambda_n$ along the diagonal.

(a) The matrix of $1 + iT$ is diagonal with nonzero complex numbers $1 + i\lambda_j$ along the diagonal, so $1 + iT$ is invertible.

(b) The matrix A of $(1 - iT)(1 + iT)^{-1}$ is diagonal with (j, j)-entry equal to $(1 - i\lambda_j)/(1 + i\lambda_j)$, which is a complex number of absolute value 1 (since numerator and denominator are complex conjugates, hence of equal absolute value). So the conjugate transpose of A is the inverse of A. This means that the corresponding linear operator is unitary.

8B. For $R > 0$ let Γ_R be the semicircle $\{|z| = R,\ \mathrm{Im} z \geq 0\}$ (radius R, center 0, in the upper half-plane). Prove that

$$\lim_{R\to\infty} \int_{\Gamma_R} \frac{e^{iz}}{z} dz = 0.$$

Solution: Parameterize $\Gamma_R : z = Re^{i\theta}$, $0 \leq \theta \leq \pi$. Then the integral above is

$$\begin{aligned} I_R &= i \int_0^\pi e^{iRe^{i\theta}} d\theta \\ &= i \int_0^\pi e^{iR\cos\theta} e^{-R\sin\theta} d\theta \end{aligned}$$

so that

$$|I_R| \leq \int_0^\pi e^{-R\sin\theta} d\theta.$$

Note that $|e^{-R\sin\theta}| \leq 1$ since $\sin\theta \geq 0$. Also, for $0 < \theta < \pi$, $e^{-R\sin\theta} \to 0$ as $R \to \infty$. Hence, by the bounded convergence theorem, $|I_R| \to 0$ as $R \to \infty$.

A proof using only Math 104 techniques: given $\varepsilon > 0$, $e^{-R\sin\theta} \to 0$ *uniformly* on the interval $[\varepsilon, \pi - \varepsilon]$. Also, for all R, $0 \leq \left(\int_0^\varepsilon + \int_{\pi-\varepsilon}^\pi\right) e^{-R\sin\theta} \leq 2\varepsilon$.

Hence for R sufficiently large,

$$0 \leq \int_0^\pi e^{-R\sin\theta} d\theta < 3\varepsilon.$$

Thus $\lim_{R\to\infty} |I_R| = 0$.

9B. Let $f\colon \mathbb{R} \to \mathbb{R}$ be a function. Prove that there exists a countable subfield K of $\mathbb{R}$ such that $f(K) \subseteq K$.

Solution: Let $E_0 = \mathbb{Z}$. For $i \geq 1$, define

$$\begin{aligned} A_i &:= \{x + y : x, y \in E_{i-1}\} \\ B_i &:= \{x - y : x, y \in A_i\} \\ C_i &:= \{xy : x, y \in B_i\} \\ D_i &:= \{x/y : x, y \in C_i \text{ and } y \neq 0\} \\ E_i &:= D_i \cup f(D_i). \end{aligned}$$

Each set is contained in the next. Since finite unions, finite products, subsets, and images of countable sets are countable, induction shows that all these sets are countable. Let $K = \bigcup_{i=0}^{\infty} E_i$, which again is countable.

We claim that K is closed under addition. Suppose $x, y \in K$. Then $x \in E_i$ for some i, and $y \in E_j$ for some j. Without loss of generality, suppose $j \geq i$. Then $x, y \in E_j$, so $x + y \in A_{j+1} \subseteq E_{j+1} \subseteq K$.

Similarly, K is closed under subtraction, multiplication, and division (by nonzero elements of K), so K is a subfield of $\mathbb{R}$. And similarly, K is closed under f.

Alternative solution: Let K be the set of real numbers that can be obtained in a finite sequence of steps from 0 and 1 using the operations of addition, subtraction, multiplication, division, and applying f. Clearly K is a field, and $f(K) \subseteq K$. It remains to prove that K is countable.

For each $x \in K$, choose a representation of x by a formula in TeX, such as

```
\frac{f(f(1+1)/f(0))-f(1)}{f(1+f(1))}+1
```

representing

$$\frac{f(f(1+1)/f(0)) - f(1)}{f(1+f(1))} + 1$$

The formula is a finite string of typewriter symbols, and if we encode each symbol by a 3-digit integer between 100 and 999, and concatenate, we obtain a long integer x'. The association $x \mapsto x'$ defines an injection $K \hookrightarrow \mathbb{N}$, so K is countable.