Solutions to the Spring 2003 prelim

1A. Let $k$ be a field, and let $n \geq 1$. Prove that the following properties of an $n \times n$ matrix $A$ with entries in $k$ are equivalent:

(a) $A$ is a scalar multiple of the identity matrix.

(b) Every nonzero vector $v \in k^n$ is an eigenvector of $A$.

Solution: Obviously (a) implies (b). If (b) holds, then in particular, the standard basis vectors $e_j$ are eigenvectors of $A$, so $A$ is diagonal, say with entries $A_{ii} = \lambda_i$. If $\lambda_i \neq \lambda_j$, then $A(e_i + e_j) = \lambda_i e_i + \lambda_j e_j$ is not a scalar multiple of $e_i + e_j$. This contradicts the hypothesis that $e_i + e_j$ is an eigenvector of $A$. Hence the diagonal entries $\lambda_i$ are all equal and we have (a).

2A. Define $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(x, 0) = 0$ and

$$f(x,y) = \left(1 - \cos\frac{x^2}{y}\right)\sqrt{x^2+y^2}$$

for $y \neq 0$.

(a) Show that $f$ is continuous at $(0, 0)$.

(b) Calculate all the directional derivatives of $f$ at $(0, 0)$.

(c) Show that $f$ is not differentiable at $(0, 0)$.

Solution:

(a) We have $|f(x, y)| \leq 2\sqrt{x^2 + y^2}$, and the latter tends to 0 as $(x, y) \to (0, 0)$.

(b) In the direction of $(x, y)$ with $y \neq 0$, the directional derivative is

$$\lim_{t\to 0}\frac{f(tx,ty)}{t} = \lim_{t\to 0}\left(1 - \cos\frac{t^2x^2}{ty}\right)\sqrt{x^2+y^2} = 0,$$

and the limit is trivially zero in the direction of $(x, 0)$ for any $x$.

(c) If $f$ were differentiable, the derivative would be zero, and then $f(x, y)/\sqrt{x^2 + y^2} \to 0$ as $(x, y) \to (0, 0)$. This is false, since if we approach $(0, 0)$ along the curve $x^2/y = \pi$, the limit of $f(x, y)/\sqrt{x^2 + y^2}$ is $1 - \cos\pi = 2$.

3A. Let $M_2(\mathbb{Q})$ denote the ring of $2 \times 2$ matrices with entries in $\mathbb{Q}$. Let $R$ be the set of matrices in $M_2(\mathbb{Q})$ that commute with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

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

(b) Prove that $R$ is isomorphic to the ring $\mathbb{Q}[x]/(x^2)$.

Solution:

(a) Let $N = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $A, B \in R$, then $(A+B)N = AN+BN = NA+NB = N(A+B)$, so $A + B \in R$. If $A, B \in R$, then $(AB)N = A(BN) = A(NB) = (AN)B = (NA)B = N(AB)$, so $AB \in R$. If $I$ is the identity matrix, then clearly $-I \in R$. These three facts imply that $R$ is a subring.

(b) Calculating shows that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to $R$ if and only if $a = a + c$, $a + b = b + d$, and $c + d = d$, that is, if and only if $A$ has the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$. We define a $\mathbb{Q}$-algebra homomorphism $h : \mathbb{Q}[x] \to R$ by mapping $x$ to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Clearly $h(x^2) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$, so $h$ induces a homomorphism $\mathbb{Q}[x]/(x^2) \to R$. Since $h(a + bx) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, this homomorphism $\mathbb{Q}[x]/(x^2) \to R$ is an isomorphism.

4A. Prove that for each integer $n \geq 0$ there is a polynomial $T_n(x)$ with integer coefficients such that the identity

$$2 \cos nz = T_n(2 \cos z)$$

holds for all $z$.

Solution: Put $q = e^{iz}$, so $2 \cos z = q + q^{-1}$, and $2 \cos nz = q^n + q^{-n}$. Then the problem is to find $T_n$ such that $T_n(q + q^{-1}) = q^n + q^{-n}$. We have

$$(q+q^{-1})^n = \sum_{k=0}^{n} \binom{n}{k} q^{2k-n} = q^n + q^{-n} + \sum_{\substack{0<j<n \\ n-j \text{ even}}} \binom{n}{(n-j)/2} (q^j + q^{-j}) + \begin{cases} \binom{n}{n/2} & \text{if } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

We can assume we have found $T_j$ for $j < n$ by induction. Then

$$T_n(x) = x^n - \sum_{\substack{0<j<n \\ n-j \text{ even}}} \binom{n}{(n-j)/2} (T_j(x)) - \begin{cases} \binom{n}{n/2} & \text{if } n \text{ is even,} \\ 0 & \text{otherwise} \end{cases}$$

has the required property.

5A. Let $L$ be a real symmetric $n \times n$ matrix with 0 as a simple eigenvalue, and let $v \in \mathbb{R}^n$.

(a) Show that for sufficiently small positive real $\epsilon$, the equation $Lx + \epsilon x = v$ has a unique solution $x = x(\epsilon) \in \mathbb{R}^n$.

(b) Evaluate $\lim_{\epsilon \to 0^+} \epsilon x(\epsilon)$ in terms of $v$, the eigenvectors of $L$, and the inner product $( \, , \, )$ on $\mathbb{R}^n$.

Solution: Since $L$ is real and symmetric, $\mathbb{R}^n$ has an orthonormal basis of eigenvectors $e_1, \ldots, e_n$ of $L$. Let $\lambda_1, \ldots, \lambda_n$ be the associated eigenvalues. Without loss of generality, $\lambda_1 = 0$ and $\lambda_i \neq 0$ for $i > 1$. Write $v = \sum_{i=1}^n v_i e_i$ and $x = \sum x_i e_i$ with $v_i, x_i \in \mathbb{R}$. The equation $Lx + \epsilon x = v$ is equivalent to $\lambda_i x_i + \epsilon x_i = v_i$ for each $i$, which has the unique solution $x_i = v_i/(\lambda_i + \epsilon)$, provided that $0 < \epsilon < \min_{i \neq 1} |\lambda_i|$. Now

$$\epsilon x = \sum \epsilon x_i e_i = \sum \frac{\epsilon}{\lambda_i + \epsilon} v_i e_i.$$

As $\epsilon \to 0$, all terms in the sum on the right tend to 0 except the first, which tends to $v_1 e_1 = (v, e_1) e_1$.

6A. Let $x_n$ be a sequence of real numbers so that $\lim_{n \to \infty}(2x_{n+1} - x_n) = x$. Show that $\lim_{n \to \infty} x_n = x$.

Solution: First show that $\{x_n\}$ is bounded. We know that the sequence $\{2x_{n+1} - x_n\}$ is bounded. Then we can choose $M$ large so that $|x_1| \leq M$ and $|2x_{n+1} - x_n| \leq M$ for all $n$. We prove by induction that $|x_n| \leq M$ for all $n$. Indeed, suppose that $|x_n| \leq M$. Then

$$|x_{n+1}| = |\frac{x_n + (2x_{n+1} - x_n)}{2}| \leq \frac{1}{2}(|x_n| + |2x_{n+1} - x_n|) \leq M$$

This concludes the induction and shows that $\{x_n\}$ is bounded.

Now write again

$$x_{n+1} = \frac{x_n + (2x_{n+1} - x_n)}{2}$$

and take lim sup. We get

$$\limsup x_n \leq \frac{\limsup x_n + x}{2}$$

which gives $\limsup x_n \leq x$. Similarly we get $\liminf x_n \geq x$. Together these two inequalities imply that $\lim x_n = x$.

7A. (a) Suppose that $H_1$ and $H_2$ are subgroups of a group $G$ such that $H_1 \cup H_2$ is a subgroup of $G$. Prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

(b) Show that for each integer $n \geq 3$, there exists a group $G$ with subgroups $H_1$, $H_2$, ..., $H_n$, such that no $H_i$ is contained in any other, and such that $H_1 \cup H_2 \cup \cdots \cup H_n$ is a subgroup of $G$.

Solution:

(a) If not, there exists $h_1 \in H_1 - H_2$ and $h_2 \in H_2 - H_1$. Since $h_1$ and $h_2$ belong to the subgroup $H_1 \cup H_2$, we also have $h_1 h_2 \in H_1 \cup H_2$. If $h_1 h_2 \in H_1$, we get the contradiction $h_2 = h_1^{-1}(h_1 h_2) \in H_1$. If $h_1 h_2 \in H_2$, we get the contradiction $h_1 = (h_1 h_2) h_2^{-1} \in H_2$.

(b) Let $G = (\mathbb{Z}/2\mathbb{Z})^{n-1}$. For $1 \leq i \leq n-1$, let $H_i = \{\, (x_1, \ldots, x_{n-1}) \in G : x_i = 0 \,\}$. Then $H_1 \cup \cdots \cup H_{n-1} = G - \{(1, 1, \ldots, 1)\}$. Let $H_n = \{\, (x_1, \ldots, x_{n-1}) \in G : x_1 + x_2 = 0 \,\}$. Then $(1, 1, \ldots, 1) \in H_n$, so $H_1 \cup \cdots \cup H_n = G$. No $H_i$ is contained in any other, since they are distinct subgroups of the same order.

8A. Evaluate $\int_0^\infty e^{-x^2} \cos x^2 \, dx$.

Solution: It is the real part of

$$I := \int_0^\infty e^{-(1+i)x^2} \, dx = \int_0^\infty e^{-\sqrt{2} e^{i\pi/4} x^2} \, dx = \int_0^\infty e^{-\sqrt{2}(e^{i\pi/8} x)^2} \, dx.$$

Let $C$ denote the wedge-shaped closed contour consisting of the straight path from 0 to $R > 0$, the arc $\gamma$ given by $e^{it} R$ as $t$ goes from 0 to $\pi/8$, and the straight path from $e^{i\pi/8} R$ to 0. By Cauchy's Theorem, $\int_C e^{-\sqrt{2} z^2} \, dz = 0$. But $\int_\gamma e^{-\sqrt{2} z^2} \, dz \to 0$ as $R \to \infty$, since the integrand is bounded in absolute value by $|e^{-\sqrt{2} e^{i\pi/4} R^2}| = e^{-R^2}$ along $\gamma$, while the length of $\gamma$ is $O(R)$. Thus $\int_C e^{-\sqrt{2} z^2} \, dz = 0$ implies

$$0 = \int_0^\infty e^{-\sqrt{2} z^2} \, dz - \int_0^\infty e^{-\sqrt{2}(e^{i\pi/8} x)^2} \, d(e^{i\pi/8} x)$$

or equivalently,

$$0 = 2^{-1/4} \int_0^\infty e^{-u^2} \, du - e^{i\pi/8} I,$$

so $I = 2^{-1/4}e^{-i\pi/8}\frac{\sqrt{\pi}}{2}$. Thus the answer, which is the real part of $I$, is

$$2^{-5/4}(\cos \pi/8)\sqrt{\pi}.$$

9A. Let $R$ be the set of complex numbers of the form

$$a + 3bi, \quad a, b \in \mathbb{Z}.$$

Prove that $R$ is a subring of $\mathbb{C}$, and that $R$ is an integral domain but not a unique factorization domain.

Solution: It's routine to verify that $R$ is an additive subgroup and is closed under multiplication. Since $\mathbb{C}$ is a field, any subring is an integral domain. Consider two factorizations of the integer 10 in $R$, namely $10 = 2 \cdot 5$ and $10 = (1+3i)(1-3i)$. The norm $|z|^2 = a^2 + 9b^2$ of any $z \in R$ is an integer, and if $|z|^2 < 9$ then $b = 0$, so $z$ is a real integer. This implies in particular that 2 has no non-trivial factorization in $R$. If $R$ were a UFD, then 2 would divide $1+3i$ or $1-3i$. But that can't be, since $(1 \pm 3i)/2$ are not in $R$.

1B. (a) Prove that there is no continuously differentiable, measure-preserving bijective function $f \colon \mathbb{R} \to \mathbb{R}_{>0}$.

(b) Find an example of a continuously differentiable, measure-preserving bijective function $f \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}_{>0}$.

Solution: For either (a) or (b), the measure-preserving condition is that the Jacobian determinant $J(f)$ has absolute value 1 everywhere. By continuity, we must have $J(f) = 1$ or $J(f) = -1$ identically. In (a), this would mean $f'(x) = 1$ or $f'(x) = -1$, so $f(x) = c + x$ or $f(x) = c - x$. Thus $f$ cannot map $\mathbb{R}$ into $\mathbb{R}_{>0}$. One possible example for (b) is $f(x, y) = (e^{-y}x, e^y)$.

2B. For an analytic function $h$ on $\mathbb{C}$, let $h^{(i)}$ denote its $i$-th derivative. (If $i = 0$, then $h^{(i)} = h$.) Suppose that $f$ and $g$ are analytic functions on $\mathbb{C}$ satisfying

$$f^{(n)} + a_{n-1}f^{(n-1)} + \cdots + a_0 f^{(0)} = 0$$
$$g^{(m)} + b_{m-1}g^{(m-1)} + \cdots + b_0 g = 0$$

for some constants $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{m-1} \in \mathbb{C}$. Show that the product function $F = fg$ satisfies

$$c_{mn}F^{(mn)} + c_{mn-1}F^{(mn-1)} + \cdots + c_0 F = 0$$

for some constants $c_0, \ldots, c_{mn} \in \mathbb{C}$ not all zero.

Solution: By induction on $k$, the function $F^{(k)}$ is a linear combination of the $mn$ functions $f^{(i)}g^{(j)}$ for $0 \le i < n$, $0 \le j < m$, with constant coefficients. Therefore the $mn + 1$ functions $F^{(0)}, \ldots, F^{(mn)}$ are linearly dependent over $\mathbb{C}$.

3B. Let $f$ be an entire function such that $\operatorname{Re} f(z) \ge -2$ for all $z \in \mathbb{C}$. Show that $f$ is constant.

Solution: The function $g(z) = e^{-f(z)}$ is entire, and $|g(z)| = e^{-\operatorname{Re} f(z)} \le e^2$. Liouville's Theorem implies that $g$ is constant, say $g(z) = c$. Clearly $c \ne 0$. Then $f$ maps the connected set $\mathbb{C}$ into the discrete set of all logarithms of $c$, so $f$ is constant.

4B. Suppose $G$ is a nonabelian simple group, and $A$ is its automorphism group. Show that $A$ contains a normal subgroup isomorphic to $G$.

Solution: For $g$ in $G$, let $c_g : G \to G$ be the inner automorphism $c_g(h) = ghg^{-1}$. Then it is easy to check that $g \mapsto c_g$ defines a homomorphism $G \to A$. It is nontrivial since $G$ is nonabelian, and thus an injection since $G$ is simple. Let $B$ be the image, so $B \simeq G$. If $\alpha \in A$ and $g, h \in G$, then

$$\alpha(c_g(h)) = \alpha(ghg^{-1}) = \alpha(g)\alpha(h)\alpha(g)^{-1} = c_{\alpha(g)}(\alpha(h)),$$

so $\alpha \circ c_g = c_{\alpha(g)} \circ \alpha$ in $A$. Thus $\alpha \circ c_g \circ \alpha^{-1} = c_{\alpha(g)}$, so $B$ is normal in $G$.

5B. Let $C$ and $D$ be nonempty closed subsets of $\mathbb{R}^n$, and assume that $C$ is bounded. Prove that there exist points $x_0 \in C$ and $y_0 \in D$ such that $d(x_0, y_0) \leq d(x, y)$ for all $x \in C$, $y \in D$. Here $d(x, y)$ denotes the Euclidean metric on $\mathbb{R}^n$.

Solution: It follows from the triangle inequality that $d(x, y)$ is uniformly continuous as a real-valued function on $C \times D$. If $C$ and $D$ were both bounded, then $C \times D$ would be compact and $d(x, y)$ would attain its minimum. In the general case, let $d_0$ be the infimum of $d(x, y)$ on $C \times D$. Let $B_{R_0}$ be a closed ball of radius $R_0$ around the origin containing $C$, and set $R_1 = R_0 + d_0 + \epsilon$, for some arbitrary $\epsilon > 0$. Then for $y \notin B_{R_1}$, we clearly have $d(x, y) > d_0 + \epsilon$ for all $x \in C$. It follows that $D \cap B_{R_1}$ is non-empty, and the infimum of $d(x, y)$ on $C \times (D \cap B_{R_1})$ is equal to $d_0$. Since $C \times (D \cap B_{R_1})$ is compact, the minimum is attained for some $(x_0, y_0) \in C \times (D \cap B_{R_1})$.

6B. Let $\mathrm{GL}_2(\mathbb{C})$ denote the group of invertible $2 \times 2$ matrices with coefficients in the field of complex numbers. Let $\mathrm{PGL}_2(\mathbb{C})$ denote the quotient of $\mathrm{GL}_2(\mathbb{C})$ by the normal subgroup $\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{C}^* \right\}$. Let $n$ be a positive integer, and suppose that $a, b$ are elements of $\mathrm{PGL}_2(\mathbb{C})$ of order exactly $n$. Prove that there exists $c \in \mathrm{PGL}_2(\mathbb{C})$ such that $cac^{-1}$ is a power of $b$.

Solution: Choose $A \in \mathrm{GL}_2(\mathbb{C})$ representing $a$. Then $A^n = \lambda I$ for some $\lambda \in \mathbb{C}^*$. By dividing $A$ by an $n$-th root of $\lambda$, we may assume without loss of generality that $A^n = I$. Since the polynomial $x^n - 1$ has distinct roots, $A$ is diagonalizable, and the eigenvalues must be $n$-th roots of unity. Without loss of generality, we may conjugate, and divide $A$ by the first root of unity, to assume that $A = \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$. If for some $m \geq 1$, $A^m = sI$ for some $s \in \mathbb{C}^*$, then comparing upper left hand corners shows that $s = 1$. Since the order of $a$ is exactly $n$, the previous sentence implies that $A$ has order exactly $n$, so that $\zeta$ is a primitive $n$-th root of unity.

Similarly, $b$ is represented by a matrix that is conjugate to $B = \begin{pmatrix} 1 & 0 \\ 0 & \zeta' \end{pmatrix}$ for some primitive $n$-th root of unity $\zeta'$. Then $\zeta'$ is a power of $\zeta$, so $B$ is a power of $A$, and $b$ is conjugate to a power of $a$.

7B. Let $f(z)$ be a function that is analytic in the unit disk $D = \{|z| < 1\}$. Suppose that $|f(z)| \leq 1$ in $D$. Prove that if $f(z)$ has at least two fixed points $z_1$ and $z_2$ (that is, $f(z_j) = z_j$ for $j = 1, 2$), then $f(z) = z$ for all $z \in D$.

Solution: Let $S$ be a linear fractional transformation which maps $D$ onto itself so that $S(0) = x_1$. Then $g = S^{-1} \circ f \circ S$ has the same properties as $f$ and its two fixed points are $0 = S^{-1}(z_1)$ and $y = S^{-1}(z_2)$.

Since $g(0) = 0$ we can define the analytic function $h(z) = g(z)/z$. On the circle $|z| = 1 - \epsilon$ for fixed $\epsilon \in (0, 1)$, we have $|h(z)| = |g(z)|/|z| \leq 1/(1 - \epsilon)$, so the maximum principle implies $|h(z)| \leq 1/(1 - \epsilon)$ for $|z| \leq 1 - \epsilon$. This holds for arbitrarily small $\epsilon > 0$, so $|h(z)| \leq 1$ for all $z \in D$.

On the other hand we know that $h(y) = 1$, so $h$ assumes a maximum inside $D$. By the maximum principle $h$ must be constant; that is, $h = 1$. This implies that $g(z) = z$ and then $f(z) = z$.

8B. Let $N = 30030$, which is the product of the first six primes. How many nonnegative integers $x$ less than $N$ have the property that $N$ divides $x^3 - 1$?

Solution: We want the number of solutions to $x^3 = 1$ in the ring $\mathbb{Z}/N\mathbb{Z}$. By the Chinese Remainder Theorem, $\mathbb{Z}/N\mathbb{Z}$ is isomorphic as a ring to $\prod_{p \in \{2,3,5,7,11,13\}} \mathbb{Z}/p\mathbb{Z}$. Thus the answer is $\prod_{p \in \{2,3,5,7,11,13\}} n_p$, where $n_p$ is the number of solutions to $x^3 - 1$ in $\mathbb{Z}/p\mathbb{Z}$. Now $n_p$ is the number of elements of order dividing 3 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$, we have $n_p = 3$ if 3 divides $p - 1$, and $n_p = 1$ otherwise. Thus the answer is

$$n_2 n_3 n_5 n_7 n_{11} n_{13} = 1 \cdot 1 \cdot 1 \cdot 3 \cdot 1 \cdot 3 = 9.$$

9B. Let $A \subseteq \mathbb{R}$ be uncountable.

(a) Show that $A$ has at least one accumulation point.

(b) Show that $A$ has uncountably many accumulation points.

(Recall that a point is said to be an accumulation point of $A$ if and only if it is the limit of a sequence of distinct terms from $A$.)

Solution:

(a) For $n \in \mathbb{Z}$ let $A_n = A \cap [n, n+1)$. Then $A = \cup_{n \in \mathbb{Z}} A_n$. Since $A$ is uncountable, at least one of the sets $A_n$ needs to be uncountable. Then we can find a sequence in $A_n$ with distinct terms. This sequence is bounded, so it has a convergent subsequence. The limit of the subsequence is an accumulation point for $A$.

(b) Denote by $B$ the set of accumulation points. Assume by contradiction that $B$ is at most countable. The set $B$ is closed, so its complement $\mathbb{R} \setminus B$ is open. Then we can represent it as a countable union of closed sets, $\mathbb{R} \setminus B = \cup C_n$. If $B$ is at most countable then $A$ must have uncountably many elements in $\mathbb{R} \setminus B$, therefore in one of the sets $C_n$. By part (a), $A \cap C_n$ has at least one accumulation point. $C_n$ is closed, so this accumulation point is in $C_n$. This contradicts the fact that all accumulation points of $A$ are in $B$ which does not intersect $C_n$.