

**SPRING 2005 PRELIMINARY EXAMINATION SOLUTIONS**

1A. (a) Let  $(a_n)_1^\infty$  be a sequence in  $\mathbb{R}$  such that

$$\sum_{n=1}^{\infty} |a_{n+1} - a_n| < \infty.$$

Prove that  $(a_n)_1^\infty$  is a Cauchy sequence.

(b) Is the converse true? Give a proof or a counterexample.

Solution: (a) Given  $\varepsilon > 0$ , there is an integer  $N$  such that

$$\sum_{k=N}^{\infty} |a_{k+1} - a_k| < \varepsilon.$$

Therefore, for any  $m, n$  with  $N \leq m < n$ ,

$$\left| \sum_{k=m}^{n-1} (a_{k+1} - a_k) \right| \leq \sum_{k=m}^{n-1} |a_{k+1} - a_k| < \varepsilon.$$

The series on the left telescopes, giving

$$|a_n - a_m| < \varepsilon.$$

(b) Simple counterexample:  $a_n = (-1)^n/n$ . Then  $|a_{n+1} - a_n| = (2n+1)/(n^2+n)$ , so  $\sum_{n=1}^{\infty} |a_{n+1} - a_n| = \infty$  by the limit comparison test (compare with  $\sum_{n=1}^{\infty} \frac{1}{n}$ ).

2A. Prove or disprove the statement: Every function  $f: \mathbb{R} \rightarrow \mathbb{R}$  such that  $f(x+y) = f(x) + f(y)$  for all  $x$  and  $y$  is continuous.

Solution: The statement is false. Let  $\pi$  be an irrational number. Then 1 and  $\pi$  are linearly independent over  $\mathbb{Q}$ , so we may extend the set  $\{1, \pi\}$  to a basis  $B$  of  $\mathbb{R}$  as a  $\mathbb{Q}$ -vector space. There exists a  $\mathbb{Q}$ -linear function  $f: \mathbb{R} \rightarrow \mathbb{Q}$  taking arbitrarily prescribed values on the basis  $B$ ; choose  $f$  such that  $f(1) = 1$ ,  $f(\pi) = 0$ . The first condition implies  $f(x) = x$  for all  $x \in \mathbb{Q}$ . If  $f$  were continuous it would follow that  $f(x) = x$  for all  $x \in \mathbb{R}$ , contradicting  $f(\pi) = 0$ .

3A. Prove that there is no holomorphic bijection from the punctured disk  $0 < |z| < 1$  in  $\mathbb{C}$  onto the annulus  $r < |z| < R$ , where  $0 < r < R < \infty$ .

Solution: Suppose the analytic function  $f$  maps  $D \setminus \{0\} = \{z : 0 < |z| < 1\}$  onto the annulus  $A$ . Then  $f$  is bounded in a neighborhood of 0, and therefore  $f$  has a removable singularity at 0, so  $f$  extends to an analytic function on the open disk  $D$ . By the open mapping theorem,  $f(0) = p \in A$ . Also there is some  $z_0 \in D \setminus \{0\}$  with  $f(z_0) = p$ . Then there are small disjoint neighborhoods  $U, V$  of 0 and  $z_0$  respectively, such that  $f(U)$  and  $f(V)$  are neighborhoods of  $p$ .

Hence  $f(U \setminus \{0\})$  and  $f(V)$  are open sets in  $A$  which are not disjoint.

This shows that  $f$  is *not* 1-1 on  $D \setminus \{0\}$ .

4A. Suppose  $A$  and  $B$  are commuting  $n \times n$  matrices over  $\mathbb{R}$ . Suppose  $A$  and  $B$  are each diagonalizable over  $\mathbb{R}$ . Show that  $AB$  is diagonalizable over  $\mathbb{R}$ .

Solution: Let  $V_1, \dots, V_r$  be the eigenspaces in  $K^n$  corresponding to the distinct eigenvalues of  $A$  in  $K$ . Because  $A$  is diagonalizable,

$$K^n = \bigoplus_i V_i.$$

Because  $A$  and  $B$  commute,  $BV_i \subseteq V_i$ . Because  $B$  is diagonalizable over  $\mathbb{R}$ , its minimal polynomial is a product of linear factors over  $\mathbb{R}$ , and the minimal polynomial of  $B|_{V_i}$  divides this, so  $B|_{V_i}$  is diagonalizable as well. Thus

$$V_i = \bigoplus_j W_{ij},$$

where the  $W_{ij}$  are the eigenspaces of  $B$  in  $V_i$  corresponding to distinct eigenvalues. Since  $W_{ij}$  is an eigenspace for  $AB$  and

$$\bigoplus_{ij} W_{ij} = K^n,$$

$AB$  must be diagonalizable.

5A. Let  $I$  be an open interval and let  $f: I \rightarrow \mathbb{R}$  have continuous  $k$ -th derivatives everywhere on  $I$  for all  $k \leq n-1$ . Let  $a \in I$  be such that  $f^{(k)}(a) = 0$  for  $1 \leq k \leq n-1$ , and assume that  $f^{(n)}(a)$  is defined and  $f^{(n)}(a) > 0$ . Prove that if  $n$  is even, then  $f$  has a local minimum at  $a$ , and if  $n$  is odd, then  $f$  has no local extremum at  $a$ .

Solution: By the definition of derivative and the assumption that  $f^{(n-1)}(a) = 0$ ,

$$\lim_{x \rightarrow a} \frac{f^{(n-1)}(x)}{x-a} = f^{(n)}(a) > 0.$$

Hence there exists  $\epsilon$  such that  $f^{(n-1)}(x)/(x-a) > 0$  for all  $x \in (a-\epsilon, a+\epsilon) - \{a\}$ . By Taylor's theorem with remainder, we have

$$f(x) = f(a) + f^{(n-1)}(c)(x-a)^{n-1}/(n-1)!$$

for some  $c \in [a, x]$  if  $x \geq a$ , or  $c \in [x, a]$  if  $x \leq a$ . For  $x \in (a-\epsilon, a)$  we have  $f^{(n-1)}(c) \leq 0$ , so  $f(x) \geq f(a)$  if  $n$  is even,  $f(x) \leq f(a)$  if  $n$  is odd. For  $x \in (a, a+\epsilon)$ , we have  $f^{(n-1)}(c) \geq 0$ , so  $f(x) \geq f(a)$  for all  $n$ . This implies that  $f$  has a local minimum at  $a$  if  $n$  is even. If  $n$  is odd, it implies that either  $f$  has no local extremum, or  $f$  is constant on  $(a-\epsilon, a+\epsilon)$ . But the latter possibility contradicts the assumption that  $f^{(n)}(a) > 0$ .

6A. For every positive integer  $n$ , define  $[n]_q = q^{n-1} + q^{n-2} + \dots + q + 1$ . Prove that  $[1]_q [2]_q \cdots [r]_q$  divides  $[k+1]_q [k+2]_q \cdots [k+r]_q$  in the polynomial ring  $\mathbb{Z}[q]$ , for all positive integers  $k$  and  $r$ .

Solution: Both polynomials are monic, so we need only show that every complex root  $\omega$  of  $[1]_q [2]_q \cdots [r]_q$  is also a root of  $[1]_q [2]_q \cdots [k+r]_q$ , with equal or greater multiplicity.

The roots of  $[n]_q = (q^n - 1)/(q - 1)$  are the  $n$ -th roots of unity, excluding 1, and they are distinct. In particular, every root  $\omega$  of  $[1]_q [2]_q \cdots [r]_q$  is a root of unity. Let  $d$  be the order of  $\omega$  in the multiplicative group  $\mathbb{C}^*$ , that is,  $\omega$  is a primitive  $d$ -th root of unity. Then  $\omega$  is a root

of  $[n]_q$  if and only if  $d \mid n$ . It follows that  $\omega$  has multiplicity  $\lfloor r/d \rfloor$  as a root of  $[1]_q[2]_q \cdots [r]_q$ , and multiplicity  $\lfloor (k+r)/d \rfloor - \lfloor k/d \rfloor$  as a root of  $[k+1]_q[k+2]_q \cdots [k+r]_q$ . To complete the proof, we need the following inequality.

*Lemma.*  $\lfloor (k+r)/d \rfloor \geq \lfloor k/d \rfloor + \lfloor r/d \rfloor$  for all  $k, r, d$ .

*Proof.* Set  $a = \lfloor k/d \rfloor$ ,  $b = \lfloor r/d \rfloor$ . Then  $k \geq ad$ ,  $r \geq bd$ , hence  $k+r \geq (a+b)d$  and  $\lfloor (k+r)/d \rfloor \geq \lfloor (a+b)d/d \rfloor = a+b$ , since the floor function is monotone.

(An alternative proof is to show by induction that the Gauss binomial coefficient

$$\begin{bmatrix} k+r \\ r \end{bmatrix}_q := \frac{[k+1]_q[k+2]_q \cdots [k+r]_q}{[1]_q[2]_q \cdots [r]_q}$$

is a polynomial, by using a  $q$ -analog of the Pascal's triangle recurrence.)

7A. Let  $U$  be a connected open subset of  $\mathbb{C}$ , and let  $f(z)$  be a meromorphic function on  $U$  having at least one pole. For each  $c \in U$  that is not a pole of  $f$ , let  $R(c)$  be the radius of convergence of the Taylor series of  $f$  centered at  $c$ . Prove that  $R(c)$  extends to a continuous function defined on all of  $U$ .

Solution: Let  $P$  be the set of poles of  $f$  in  $U$ . Each pole is isolated, so  $P$  is closed in  $U$ , and  $U - P$  is open (both in  $U$  and in  $\mathbb{C}$ ). For  $c \in \mathbb{C}$  and  $r > 0$ , let  $D(c, r) := \{z \in \mathbb{C} : |z - c| < r\}$ .

Fix  $c \in U - P$ . Choose  $\epsilon > 0$  such that  $D(c, \epsilon) \subseteq U - P$ . Then  $\epsilon \leq R(c)$ , and the function  $g_c$  on  $D(c, R(c))$  defined by the Taylor series at  $c$  agrees with  $f$  on  $D(c, \epsilon)$ . Note that  $R(c) < \infty$ , since otherwise by connectedness  $f$  would equal the restriction to  $U$  of an entire function  $g_c$ , contradicting the fact that  $f$  has a pole. If  $c' \in D(c, \epsilon/2)$ , then  $\{c, c'\} \subseteq D(c', \epsilon/2) \subseteq D(c, \epsilon)$ , so the restrictions of  $g_c$  and the analogous function  $g_{c'}$  to  $D(c', \epsilon/2)$  each agree with the restriction of  $f$ . Thus  $g_c, g_{c'}, f$  have the same Taylor series centered at  $c$ , and they have the same Taylor series centered at  $c'$ . The restriction of  $g_c$  to  $D(c', R(c) - |c - c'|) \subseteq D(c, R(c))$  is holomorphic, so  $R(c') \geq R(c) - |c - c'|$ . Similarly  $R(c) \geq R(c') - |c - c'|$ , so  $|R(c) - R(c')| \leq |c - c'|$ . Thus  $R$  is continuous at  $c$ .

Suppose  $p \in P$ . We may choose  $\epsilon > 0$  such that  $D(p, \epsilon) - \{p\} \subseteq U - P$ . For  $c \in D(p, \epsilon/2) - \{p\}$ , the restriction of  $g_c$  to  $D(c, |c - p|)$  agrees with  $f$ , and  $g_c(z) \rightarrow \infty$  as  $z \rightarrow p$  within  $D(c, |c - p|)$ , so  $R(c) = |c - p|$ . Thus defining  $R(p) = 0$  at each  $p \in P$  gives an extension of  $R$  to a continuous function on  $U$ .

Remark: It is not true that  $R(c)$  equals the distance from  $c$  to the complement of  $U - \{\text{poles of } f\}$  in  $\mathbb{C}$ , even if  $f$  does not extend to a larger open subset of  $\mathbb{C}$ . For example, if  $f$  is the standard branch of  $\frac{\log z}{z-100}$  on  $\mathbb{C} - \mathbb{R}_{\leq 0}$ , then  $R(-1+i) = \sqrt{2}$ , not 1.

The correct statement is that if  $c \in U$  is not a pole, then  $R(c)$  equals the radius of the largest open disk on which there is some holomorphic function that agrees with  $f$  on some open neighborhood of  $c$ .

8A. Let  $C$  and  $D$  be two  $n \times n$  positive definite Hermitian matrices over  $\mathbb{C}$  and let  $A = CD$ . Prove that all eigenvalues of  $A$  are positive real numbers.

Solution: Let  $Ax = \lambda x$ ,  $x \neq 0$ . Then  $CDx = \lambda x$ . Since  $D$  is positive definite, it is invertible, so  $Dx \neq 0$ . Let  $B^H$  denote the conjugate transpose of a matrix (or column

vector)  $B$ . Since  $C$  is positive definite,

$$0 < \langle Dx, C(Dx) \rangle = (Dx)^H C(Dx) = (Dx)^H \lambda x = \lambda x^H D^H x = \lambda x^H Dx,$$

since  $D$  is Hermitian. But  $x^H Dx > 0$  since  $D$  is positive definite. Dividing, we get  $\lambda > 0$ .

9A. Let  $f: \mathbb{R}^2 \rightarrow \mathbb{R}$  be an infinitely differentiable function that is zero outside some bounded subset of  $\mathbb{R}^2$ . Prove that

$$\lim_{\epsilon \rightarrow 0} \iint_{x^2+y^2 \geq \epsilon^2} \frac{f(x, y)}{(x + iy)^3} dx dy$$

exists.

Solution: The answer is positive. We must prove that

$$\lim_{\delta, \epsilon \rightarrow 0} \iint_{\delta^2 < x^2+y^2 < \epsilon^2} \frac{f(x, y)}{(x + iy)^3} dx dy = 0$$

We write

$$f(x, y) = a + bx + cy + O(x^2 + y^2)$$

and consider each of the three terms. For the last one we note that

$$\frac{x^2 + y^2}{|x + iy|^3} = (x^2 + y^2)^{-\frac{1}{2}}$$

which is integrable at zero. For the constant we compute

$$\iint_{\delta^2 < x^2+y^2 < \epsilon^2} \frac{1}{(x + iy)^3} dx dy = \int_0^{2\pi} \int_{\delta < r < \epsilon} r^{-2} e^{-3i\theta} dr d\theta = 0$$

For  $f(x, y) = y$  we have

$$\begin{aligned} \iint_{\delta^2 < x^2+y^2 < \epsilon^2} \frac{y}{(x + iy)^3} dx dy &= \int_0^{2\pi} \int_{\delta < r < \epsilon} r^{-1} \cos \theta e^{-3i\theta} dr d\theta \\ &= \frac{1}{2} (\ln \epsilon - \ln \delta) \int_0^{2\pi} e^{-2i\theta} + e^{-4i\theta} d\theta \\ &= 0 \end{aligned}$$

The case  $f(x, y) = x$  is similar by symmetry. This concludes the proof.

1B. Let  $G$  be a finite group. Suppose  $ab = ba$  holds whenever  $a, b \in G$  have prime power order. Prove that  $G$  is abelian.

Solution: Let  $x, y \in G$ . By the Chinese Remainder Theorem, the finite cyclic group generated by  $x$  is a product of cyclic groups of prime power order, so we can write  $x = x_1 x_2 \cdots x_m$  where each  $x_i$  has prime power order. Write  $y = y_1 y_2 \cdots y_n$  similarly. By assumption  $x_1$  commutes with each  $y_j$ , so  $x_1$  commutes with their product  $y$ . Similarly  $x_i$  commutes with  $y$  for each  $i$ , so their product  $x$  commutes with  $y$ .

2B. Prove that, for any  $\varepsilon > 0$ , the function  $f(z) = \sin z + \frac{1}{z+i}$  has infinitely many zeros in the strip  $|\operatorname{Im} z| < \varepsilon$ .

Solution: We use Rouché's theorem. Without loss of generality, assume  $\varepsilon < \pi$ . Let  $\delta$  be the minimum value of  $|\sin z|$  on the compact set  $|z| = \varepsilon$ . Since the zeros of  $\sin z$  in  $\mathbb{C}$  are

the integer multiples of  $\pi$ , we have  $\delta > 0$ . By periodicity, we have  $|\sin z| \geq \delta$  also on the circle  $C_n$  defined by  $|z - 2\pi n| = \varepsilon$  for any  $n \in \mathbb{Z}$ . On the other hand, if  $n$  is sufficiently large, then  $|\frac{1}{z+i}| < \delta$  on  $C_n$ . For such  $n$ , Rouché's theorem implies that  $f(z)$  has the same number of zeros as  $\sin z$  inside  $C_n$ , namely 1. Letting  $n$  vary, we find infinitely many zeros of  $f(z)$  inside the strip.

3B. Let  $M_n(F)$  be the ring of  $n \times n$  matrices over a field  $F$ . Prove that for every  $A \in M_n(F)$  there exists  $X \in M_n(F)$  such that  $AXA = A$ .

Solution: Let  $\phi: F^n \rightarrow F^n$  be the linear transformation defined by  $A$ . Let  $W = \ker \phi$ , and let  $V \subseteq F^n$  be a complementary subspace, such that  $F^n = W \oplus V$ . Let  $U = \text{im } \phi$ . Note that  $\dim U = \dim V = \text{rank } A$ . The restriction  $\bar{\phi}$  of  $\phi$  to  $V$  is injective, hence  $\bar{\phi}: V \rightarrow U$  is an isomorphism. Let  $\bar{\psi}: U \rightarrow V$  be its inverse, and let  $\psi$  be any extension of  $\bar{\psi}$  from  $U$  to all of  $F^n$ . Take  $X$  to be the matrix of  $\psi$ . Then for every vector  $v$  in the column space  $U$  of  $A$ , we have  $AXv = \phi\psi v = v$ , which implies  $AXA = A$ .

4B. Let  $D$  be a subset of  $\mathbb{R}$ , and let  $f: D \rightarrow \mathbb{R}$  be a function. The graph of  $f$  is the subset

$$G := \{(x, y) : x \in D, y = f(x)\}$$

of  $\mathbb{R}^2$ . Prove that if  $G$  is compact, then  $f$  is continuous.

Solution: It suffices to prove that  $f^{-1}(C)$  is closed in  $D$  for every closed subset  $C$  of  $\mathbb{R}$ . Let  $\pi_1, \pi_2$  be the coordinate projections  $\mathbb{R}^2 \rightarrow \mathbb{R}$ . Then  $\pi_2^{-1}(C)$  is closed in  $\mathbb{R}^2$ . Thus  $\pi_2^{-1}(C) \cap G$  is closed in  $G$  and hence compact. Now  $f^{-1}(C) = \pi_1(\pi_2^{-1}(C) \cap G)$  is the continuous image of a compact set, so it is compact. Thus  $f^{-1}(C)$  is closed in  $\mathbb{R}$ , hence closed in  $D$ .

5B. Let  $\mathbb{Q}(x)$  be the field of rational functions in one variable over  $\mathbb{Q}$ . Let  $i: \mathbb{Q}(x) \rightarrow \mathbb{Q}(x)$  be the unique field automorphism such that  $i(x) = x^{-1}$ . Prove that the fixed subfield  $\{r \in \mathbb{Q}(x) : i(r) = r\}$  is equal to  $\mathbb{Q}(x + x^{-1})$ .

Solution: Let  $F$  denote the fixed subfield, and set  $y = x + x^{-1}$ . Obviously  $\mathbb{Q}(y) \subseteq F \neq \mathbb{Q}(x)$ . The equation  $x^2 - yx + 1 = 0$  shows that  $\mathbb{Q}(x)$  is an algebraic extension of  $\mathbb{Q}(y)$ , and  $[\mathbb{Q}(x) : \mathbb{Q}(y)] = 2$ . Since the intermediate field  $F$  is not equal to  $\mathbb{Q}(x)$ , we must have  $F = \mathbb{Q}(y)$ .

6B. Evaluate the integral  $\int_0^\infty \frac{x \sin x}{x^2 + a^2} dx$ , where  $a > 0$ .

Solution: Let  $I$  be the desired integral. Then

$$\begin{aligned} I &= \frac{1}{2} \int_{-\infty}^{\infty} \frac{x \sin x}{x^2 + a^2} dx \\ &= \frac{1}{2} \lim_{R \rightarrow \infty} \int_{-R}^R \frac{x \sin x}{x^2 + a^2} dx \\ &= \frac{1}{2} \lim_{R \rightarrow \infty} \text{Im} \int_{-R}^R \frac{x e^{ix}}{x^2 + a^2} dx. \end{aligned}$$

Integrate  $\frac{ze^{iz}}{z^2+a^2}$  counterclockwise around the curve  $-R \leq x \leq R$ ,  $z = Re^{i\theta}$ ,  $0 \leq \theta \leq \pi$ , where  $R > a$ .

The residue of the integrand at  $z = ia$  is

$$\frac{iae^{-a}}{2ia} = \frac{e^{-a}}{2}.$$

Moreover, by “Jordan’s lemma”, the integral over the semicircular part of the curve tends to 0 as  $R \rightarrow \infty$ .

Therefore  $I = \frac{1}{2} \cdot \text{Im}(2\pi ie^{-a}/2) = \frac{\pi e^{-a}}{2}$ .

7B. Let  $\mathbb{F}_p$  be the field of  $p$  elements. Let  $\text{SL}_2(\mathbb{F}_p)$  be the group of  $2 \times 2$  matrices over  $\mathbb{F}_p$  of determinant 1. Let  $G$  be a normal subgroup of  $\text{SL}_2(\mathbb{F}_p)$ . Suppose  $G$  contains a non-identity element  $\gamma$  that fixes a nonzero vector  $v$ . Show that any  $\gamma' \in \text{SL}_2(\mathbb{F}_p)$  that fixes a nonzero vector  $v'$  belongs to  $G$ .

Solution: For each vector  $u$ , let  $S_u$  be the set of elements of  $\text{SL}_2(\mathbb{F}_p)$  that fix  $u$ . First, we can complete  $\{v\}$  to a basis  $\{v, w\}$ . With respect to this basis, the matrix of  $\gamma$  is upper-triangular and hence is

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

for some  $x \neq 0$ . Then  $S_v$  (where now  $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ) consists of the powers  $\gamma^k = \begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix}$ , so  $S_v \subseteq G$ .

Now suppose  $v' := \begin{pmatrix} a \\ c \end{pmatrix} \in \mathbb{F}_p^2 \setminus 0$ . Then we can find  $b, d \in \mathbb{F}_p$  so that  $ad - bc = 1$  (take  $d = 0$  and  $c = -1/b$  or  $c = 0$  and  $d = 1/a$ ). Thus

$$\rho := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{F}_p)$$

satisfies  $\rho v = v'$ . Now  $S_{v'} = \rho S_v \rho^{-1} \subseteq \rho G \rho^{-1} = G$ , which is what we needed to show.

Remark: Many students confused  $\text{SL}_2(\mathbb{F}_p)$ -conjugacy with similarity, which is  $\text{GL}_2(\mathbb{F}_p)$ -conjugacy.

8B. Let  $f: \mathbb{R} \rightarrow \mathbb{R}$  be differentiable on  $\mathbb{R}$ . Suppose that  $f(0) = 0$ , and that  $|f'(x)| \leq |f(x)|$  for all  $x \in \mathbb{R}$ . Prove that  $f(x) = 0$  for all  $x \in \mathbb{R}$ .

Solution: Let us show that  $f(x) = 0$  for all  $x \in [0, 1]$ . Let  $a = \max\{|f(x)| : x \in [0, 1]\}$ . We have to show that  $a = 0$ . Suppose on the contrary  $a > 0$ . Let  $E = \{x \in [0, 1] : |f(x)| = a\}$ . Then  $E$  is closed and  $\alpha = \inf E \in E$ , i.e.,  $|f(\alpha)| = a > 0 \Rightarrow \alpha > 0$  since  $f(0) = 0$ . Thus  $0 < \alpha \leq 1$  and  $|f(c)| < a$  for all  $0 \leq c < \alpha$ . We have  $a = |f(\alpha)| = |f(\alpha) - f(0)| = |f'(c)| \cdot \alpha$  (for some  $c \in (0, \alpha)$  by the Mean Value Theorem)  $\leq |f(c)| \cdot \alpha \leq |f(c)|$  (since  $0 < \alpha \leq 1$ ). This contradicts (\*). Thus  $f \equiv 0$  on  $[0, 1]$ . In particular,  $f(1) = 0$  and we can use the same argument to show  $f \equiv 0$  on  $[1, 2]$  and on every  $[n, n+1]$ ,  $n = \pm 1, \pm 2, \dots$

Alternative solution: Suppose  $f(x)$  is not identically zero. Replacing  $f(x)$  by  $\pm f(\pm x)$  we may assume that there exists  $b > 0$  such that  $f(b) > 0$ . Let  $a = \sup\{x \in [0, b] : f(x) = 0\}$ .

Thus  $f$  is positive on  $(a, b)$ . So  $f' \leq f$  on  $(a, b)$ . Thus the derivative of  $g = e^{-x}f$  is  $\leq 0$  on  $(a, b)$ . This contradicts  $g(a) = 0 < g(b)$ .

9B. (a) Prove that if  $n > 0$  is even, there does not exist  $f(x) \in \mathbb{R}[x]$  such that  $f(x)^2 - x$  is divisible by  $x^n - 1$ .

(b) For odd  $n > 0$ , find the number of  $f(x) \in \mathbb{R}[x]$  of degree  $< n$  such that  $f(x)^2 - x$  is divisible by  $x^n - 1$ .

Solution: (a) If  $f(x)^2 - x$  is divisible by  $x^n - 1$ , it is divisible by the factor  $x + 1$ , so  $f(-1)^2 - (-1) = 0$ . This is impossible since  $f(-1) \in \mathbb{R}$ .

(b) Equivalently, we must count the square roots of the image of  $x$  in  $\mathbb{R}[x]/(x^n - 1)$ . If  $n$  is odd, only one zero of  $x^n - 1$  is real, so  $x^n - 1 = (x - 1) \prod_{j=1}^{(n-1)/2} f_j(x)$  where  $f_j(x) \in \mathbb{R}[x]$  is irreducible of degree 2. Moreover, the factors are distinct, since  $x^n - 1$  shares no zeros with its derivative  $nx^{n-1}$ . By the Chinese Remainder Theorem,

$$\mathbb{R}[x]/(x^n - 1) \simeq \frac{\mathbb{R}[x]}{(x - 1)} \times \prod_{j=1}^{(n-1)/2} \frac{\mathbb{R}[x]}{(f_j(x))} \simeq \mathbb{R} \times \prod_{j=1}^{(n-1)/2} \mathbb{C}.$$

To choose a square root of the image of  $x$  is equivalent to choosing a square of the image of  $x$  in each factor. The image of  $x$  in the factor  $\mathbb{R}$  is 1, and the image in each factor  $\mathbb{C}$  is nonzero (since  $x$  has an inverse in  $\mathbb{R}[x]/(x^n - 1)$ , namely  $x^{n-1}$ ), so there are 2 choices of square root in each of the  $(n + 1)/2$  factors. Thus the answer is  $2^{(n+1)/2}$ .

Alternative solution to (b): By Lagrange interpolation, a polynomial  $f(x) \in \mathbb{C}[x]$  of degree  $< n$  is uniquely specified by its values at the  $n$ -th roots of unity. Such a specification gives a polynomial with real coefficients if and only if the prescribed values at complex conjugate roots of unity are complex conjugates. Now  $f(x)^2 - x$  is divisible by  $x^n - 1$  if and only if  $f(w)$  is a square root of  $w$  for each  $n$ -th root of unity  $w$ . We can construct such  $f$  by prescribing  $f(1) = \pm 1$  and  $f(w)$  for each  $n$ -th root of unity in the upper half plane, but then we must choose  $f(\bar{w}) = \overline{f(w)}$ . There are  $(n - 1)/2$   $n$ -th roots of unity in the upper half plane, so we have  $1 + (n - 1)/2 = (n + 1)/2$  sign choices. Thus there are  $2^{(n+1)/2}$  possibilities for  $f$ .