Spring prelim answers

1. List all the finite fields (up to isomorphism) of order less than or equal to 10. Show that the ones you list exist, and no others.

Solution: There is a unique finite field of each prime power order, so: 2, 3, 4, 5, 7, 8, 9. We show: (1) the order must be a prime power \( p^k \); (2) a field of each prime power cardinality \( q \) exists; and (3) it is unique.

(1) Let \( F \) be a finite field and \( 1 \in F \) the unit element. Since \( F \) is finite there is a positive integer \( c \) such that \( c1 = 0 \in F \). If \( c = ab \) then \( 0 = c1 = a1b1 \) so \( a1 = 0 \) or \( b1 = 0 \). So the smallest such \( c \) must be a prime \( p \), and \( F \) is then a vector space over the prime field \( F_p \), hence its cardinality is a power of \( p \).

(2) Conversely, let \( \overline{F} \) be an algebraic closure of \( F_p \). If \( q = p^k \), the set

\[
\{ x \in \overline{F} | x^q = x \}
\]

is closed under addition (since \( x^q + y^q = (x + y)^q \)), multiplication and inversion, so it is a subfield \( F_q \). Since the polynomial \( x^q - x \) has no repeated roots, the cardinality of \( F_q \) is \( q \).

(3) Since any field of cardinality \( q \) is the set of elements in its algebraic closure satisfying \( x^q = x \), the uniqueness of the algebraic closure implies uniqueness of \( F_q \).

2. (a) In the polynomial ring \( \mathbb{Z}[x] \), is the ideal generated by \( x^4 - 1 \) and \( 2x^3 - 2x \) principal?

(b) Same question in the polynomial ring \( \mathbb{Q}[x] \).

(c) Same question in the polynomial rings \( \mathbb{Z}[x, y] \) and \( \mathbb{Q}[x, y] \).

Solution: (a) No: such a generator must be of the form \((x^2 - 1)f(x)\), and then \( f(x) \) must generate the ideal \( I := (x^2 + 1, 2x) \), in particular \( f(x) \) must divide \( x^2 + 1 \) and \( 2x \), so it must be invertible, but \( I \) is non trivial, since it is contained in the kernel of the surjective homomorphism \( \mathbb{Z}[x] \to \mathbb{Z}/(2) \) sending \( x \) to 1. (b) Yes, in \( \mathbb{Q}[x] \) we can take the above \( f(x) \) to equal 1, since \( 1 = 1(x^2 + 1) - (\frac{1}{2})2x \in (x^2 + 1, 2x) \). (c) No change. (The analogue of (b) is trivial, and for (a) send \( y \) to 0.)

3. Use the \( \varepsilon-\delta \) definition to prove that the first derivative of \( f(x) = x^3 \) is \( f'(x) = 3x^2 \).
Solution: We must show that for any given $x_0$ and for all $\varepsilon > 0$, there exists $\delta > 0$ such that if $0 < |x - x_0| < \delta$ then $\left| \frac{x^3 - x_0^3}{x - x_0} - 3x_0^2 \right| < \varepsilon$. An easy computation shows that:

$$\left| \frac{x^3 - x_0^3}{x - x_0} - 3x_0^2 \right| = \left| (x^2 + x_0x + x_0^2) - 3x_0^2 \right| = \left| x^2 - x_0^2 + x_0x - x_0^2 \right| \leq |x^2 - x_0^2| + |x_0||x - x_0| \leq |x - x_0||x + x_0| + |x_0||x - x_0| \leq |x - x_0|(|x - x_0| + 2|x_0|) + |x_0||x - x_0|, \quad (1)$$

where the last inequality comes from $|x + x_0| \leq |x| + |x_0| \leq (|x - x_0| + |x_0|) + |x_0| = |x - x_0| + 2|x_0|$, since $|x| - |x_0| \leq |x - x_0|$ by the triangle inequality. Thus, choosing any $0 < \delta < \frac{-3|x_0| + \sqrt{9|x_0|^2 + 4\varepsilon}}{2}$, it follows that $\delta(|x + 2|x_0|) + |x_0||\delta = \delta^2 + 3|x_0|\delta < \varepsilon$ and hence by (1), the desired inequality $\left| \frac{x^3 - x_0^3}{x - x_0} - 3x_0^2 \right| < \varepsilon$ holds whenever $0 < |x - x_0| < \delta$.

4. Prove that for all $k \in \mathbb{N}$ there exists $\varepsilon_k > 0$ such that all $n \times n$ matrices $A$ with $\|A - \text{Id}\| < \varepsilon_k$ have a $k^{th}$ root, that is, an $n \times n$ matrix $\sqrt[k]{A}$ such that $(\sqrt[k]{A})^k = A$.

Solution: Identify the vector space of $n \times n$ matrices with $\mathbb{R}^{n^2}$, and consider the map $f(A) = A^k$. The coordinates of this map are smooth functions (polynomial) and hence $f$ is smooth. The linearization of $f$ at the identity matrix Id is given by

$$df(\text{Id})X = kX, \quad X \in \mathbb{R}^{n^2}.$$ In particular, $df(\text{Id})$ is invertible, hence by the Inverse Function Theorem, $f$ is locally invertible near Id $\in \mathbb{R}^{n^2}$. Thus, there exists $\varepsilon_k > 0$ such that if $\|A - \text{Id}\| < \varepsilon_k$, then $\sqrt[k]{A} := f^{-1}(A)$ is a $k^{th}$ root of $A$.

5. Let $N$ be a positive integer. Prove that

$$\frac{1}{2} + \log N < \sum_{k=1}^{N} \frac{1}{k} \leq 1 + \log N.$$ Solution: This is a standard problem which appears in many calculus books. A partial sum of the harmonic series can be viewed geometrically as the sum of the areas of boxes of width one and height $1, 1/2, 1/3, \ldots, 1/N$, which can be approximated by the area under the curve $y = \ln x$ from 1 to $N$. The difference is the sum of the areas of a bunch of slivers of width 1 above the graph of $y = 1/x$, together with the last box of height $1/N$. If you slide all these slivers left, they all fit in a box of width 1 and height 1, and the concavity of the graph shows that the sum of the areas of the slivers is larger than $1/2$. See for example the picture on p. 595 of Thomas’ Calculus, applied to the case $f(x) = \ln x$. 

6. For a positive integer, let \( \phi(n) \) denote the number of integers \( k \), \( 1 \leq k < n \), which are relatively prime to \( n \). Prove that
\[
\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),
\]
where the product is over all distinct primes \( p \) dividing \( n \).

Solution: We use a standard inclusion-exclusion argument. The number of integers relatively prime to \( n \) and between 1 and \( n \) is the number of integers between 1 and \( n \) (there are \( n \) of these), minus all multiples of \( p \) for each \( p \) dividing \( n \) (there are \( n/p \) of these), plus all multiples of \( pq \) for all pairs of distinct primes \( p, q \) dividing \( n \) (there are \( n/(pq) \) of these), etc., or
\[
n - \sum_{p|n} n/p + \sum_{p<q \text{ with } p,q|n} n/(pq) - \ldots = n \prod_{p|n} \left(1 - 1/p\right).
\]

7. Let
\[
A = \begin{bmatrix}
1 & 1 & 2 \\
1 & -1 & 2 \\
2 & -3 & 1 \\
0 & 1 & 3
\end{bmatrix}.
\]
Find an orthonormal basis of the column space of \( A \).

Solution: Let \( a_j \) denote the \( j \)-th column vector of \( A \). Let \( v_1 = a_1 \) and
\[
v_2 = a_2 - \frac{a_2 \cdot v_1}{\|v_1\|} v_1 = (2, 0, -1, 1)^T.
\]
Let
\[
v_3 = a_3 - \frac{a_3 \cdot v_1}{\|v_1\|} v_1 - \frac{a_3 \cdot v_2}{\|v_2\|} v_2 = (-1, 1, 0, 2)^T.
\]
Then an orthonormal basis is
\[
\left\{ \frac{1}{\sqrt{6}} (1, 1, 2, 0)^T, \frac{1}{\sqrt{6}} (2, 0, -1, 1)^T, \frac{1}{\sqrt{6}} (-1, 1, 0, 2)^T \right\}
\]

8. Let \( A \) be a \( n \times n \) matrix. Let \( \{S_1, \ldots, S_k\} \) be a collection of eigenvectors of \( A \) with \( \lambda_1, \ldots, \lambda_k \) as the corresponding eigenvalues. Prove that if \( \lambda_i \neq \lambda_j \) for all \( 1 \leq i < j \leq k \), then \( \{S_1, \ldots, S_k\} \) is linearly independent.

Solution: Suppose there are constants \( \{c_j\}_{1 \leq j \leq k} \) such that
\[
\sum_{j=1}^{k} c_j S_j = 0.
\]
For $1 \leq l \leq k$, define

$$B_l = \prod_{1 \leq j \leq k, j \neq l} (A - \lambda_j I).$$

Then

$$0 = B_l \sum_{j=1}^{k} c_j S_j = c_l \prod_{1 \leq j \leq k, j \neq l} (\lambda_l - \lambda_j) S_l.$$

Since $\lambda_i \neq \lambda_j$ for all $i \neq j$, $c_l = 0$ for all $1 \leq l \leq k$.

9. Let $(X,d)$ be a compact metric space. Suppose that $f : X \to X$ satisfies $d(f(x), f(y)) < d(x, y)$ for $x \neq y$. Show that for any $x_0 \in X$, the sequence defined by $x_0 = x$ and $x_{n+1} = f(x_n)$ converges to a unique fixed point of $f$.

Solution: If there were two fixed points $x$ and $y$, then $d(x, y) < d(x, y)$, so there is at most one. The function $d(f(x), x)$ is continuous and so achieves a minimum at some point $y$. If the minimum is not zero, then $f(y) \neq y$, in which case $d(f(y), f^2(y))$ is smaller, a contradiction. Therefore it is zero, i.e. $f(y) = y$.

The same thing applies to the closure $A$ of the set of points $\{x_1, \ldots, x_n, \ldots\}$, as this closure is also compact and invariant under $f$. So, from above, the restriction of $f$ to $A$ will have a fixed point. Hence $y \in A$. Therefore, given $\epsilon > 0$, there exists $N$ such that $d(x_N, y) < \epsilon$.

Thus the sequence converges to $y$.

10. A topological property is one that is invariant under homeomorphism, i.e. if two spaces are homeomorphic and one has the property, so does the other. Explain with a proof or counterexample which of the following properties of a metric space are or are not topological invariants: a. Compactness, b. Connectedness, c. Boundedness d. Completeness.

Solution. a. If $f : X \to Y$ is continuous and $X$ is compact, so is $f(Y)$. Namely, for any collection $\mathfrak{A}$ of open sets covering $f(X)$, the sets $f^{-1}(U), U \in \mathfrak{A}$ cover $X$. Therefore, a finite set of these, $f^{-1}U_1, \ldots, f^{-1}U_n$ also cover $X$; therefore $f(X) \subset U_1 \cup \ldots \cup U_n$. So as each of two homeomorphic spaces are the image of the other under a continuous map, if one is compact so is the other.

b. Similarly, it suffices to show that if $f : X \to Y$ is continuous and $X$ is connected, so is $f(X)$. If $f(X)$ is the disjoint union of two non-empty open sets, then the inverse images will be two non-empty disjoint open sets whose union os all of $X$. 

c. Not a topological invariant. For example, \((0,1)\) and \(\mathbb{R}\) with the usual metric are homeomorphic. Alternatively, if \((X,d)\) is a metric space, and \(d'(x,y) = \frac{d(x,y)}{1+d(x,y)}\), then \((X,d)\) and \((X,d')\) have the same topology, i.e. the identity map is a homeomorphism, and \(d'(x,y) \leq 1\).

d. \(\mathbb{R}\) is complete but \((0,1)\) is not.

11. Suppose \(f : [-1,1] \rightarrow \mathbb{R}\) is continuous on the closed interval \([-1,1]\), and twice differentiable on the open interval \((-1,1)\). Suppose also that \(f(-1) = 7\), \(f(0) = 1\) and \(f(1) = 1\). Prove that there exists \(c \in (-1,1)\) such that \(f''(c) = 6\).

Solution: The (unique) polynomial of degree two that passes through those points is

\[
p(x) = 3x^2 - 3x + 1.
\]

It follows that the function \(f - p\) vanishes at \(-1,0\) and 1. Applying Rolle’s Theorem twice, it follows that there exists a point \(c \in (-1,1)\) such that the second derivative of \(f - p\) vanishes at \(c\). Since the second derivative of \(p\) is constant equal to 6, it follows that \(f''(c) = 6\).

12. Compute the following limit if it exists and justify your conclusion:

\[
\lim_{n \rightarrow \infty} \int_0^1 (n+1)x^n(1-x^5)^{\frac{1}{2}} \, dx.
\]

Solution: Remark that the function \((1-x^5)^{\frac{1}{2}}\) is continuous on \([0,1]\) and equal to zero at \(x=1\). It follows that for every \(\varepsilon > 0\) there is a \(\delta > 0\) such that \(|(1-x^5)^{\frac{1}{2}}| = (1-x^5)^{\frac{1}{2}} < \varepsilon/2\) for \(x \in [1-\delta,1]\). On the other hand if \(x \in [0,1-\delta]\), then \(0 \leq (n+1)x^n \leq (n+1)(1-\delta)^n \rightarrow 0\) as \(n \rightarrow \infty\). It follows that there exists \(N \in \mathbb{N}\) such that \((n+1)(1-\delta)^n < \varepsilon/2\), for every \(n \geq N\). It follows that

\[
0 \leq \int_0^1 (n+1)x^n(1-x^5)^{\frac{1}{2}} \, dx = \int_0^{1-\delta} \int_0^1 (n+1)x^n(1-x^5)^{\frac{1}{2}} \, dx + \int_{1-\delta}^1 (n+1)x^n(1-x^5)^{\frac{1}{2}} \, dx \leq \varepsilon/2 + \frac{\varepsilon}{2} \int_{1-\delta}^1 (n+1)x^n \, dx \leq \varepsilon,
\]

for every \(n \geq N\). So we proved that the limit is zero.