Math GRE Subject Test Notes

Gregory Faletto

Contents

Linear Algebra

Properties of Projection Matrices

i. Formula:

$$P = A(A^TA)^{-1}A^T$$

(Note that if A is an invertible (square) matrix, then $P = A(A^TA)^{-1}A^T = AA^{-1}(A^T)^{-1}A^T = I$.)

The projection matrix projects any vector b into the column space of A. In other words, $p = Pb$ is the component of b in the column space, and the error $e = b - Pb$ is the component in the orthogonal complement. ($I - P$ is also a projection matrix. It projects b onto the orthogonal complement, and the projection is $b - Pb = e$).

(Note that if A is an invertible (square) matrix, then its column space is all of $\mathbb{R}^n$, so b is already in the column space of A.)

ii. The projection matrix is **idempotent**: it equals its square–$P^2 = P$.

iii. The projection matrix is **symmetric**: it equals its transpose–$P^T = P$.

iv. Conversely, **any symmetric idempotent matrix represents a projection**. P is unique for a given subspace.

v. If A is an $m \times n$ matrix with rank n, then $\text{rank}(P) = n$. The eigenvalues of P consist of n ones and $m - n$ zeroes. P always contains n independent eigenvectors and is thus diagonalizable.

Suppose A is a square nonsingular matrix and λ is an eigenvalue of A. Then λ^{-1} is an eigenvalue of the matrix A^{-1}.

Eigenvalues, Eigenvectors, Diagonalization, Symmetric Matrices

Notes on Diagonalization

Suppose the $n \times n$ matrix A has n linearly independent eigenvectors. If these eigenvectors are the columns of a matrix S, then $S^{-1}AS$ is a diagonal matrix Λ. The eigenvalues of A are on the diagonal of Λ:

$$S^{-1}AS = \Lambda = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

We call S the **eigenvector matrix** and Λ the **eigenvalue matrix**.

1. If the matrix A has no repeated eigenvalues, then its n eigenvectors are automatically independent. Therefore **any matrix with n distinct eigenvalues can be diagonalized**.

2. **The diagonalizing matrix S is not unique**. An eigenvector x can be multiplied by a constant and remains an eigenvector. We can multiply the columns of S by any nonzero constants and produce a new diagonalizing S. Repeated eigenvalues leave even more freedom in S (columns with identical eigenvalues can be interchanged).

   (Note that for the trivial example $A = I$, any invertible S will do. $S^{-1}IS$ is always diagonal, and Λ is just I. **All vectors are eigenvectors of the identity.**)

3. **Other matrices S will not produce a diagonal Λ**. Since $\Lambda = S^{-1}AS$, S must satisfy $S\Lambda = AS$. Suppose the first column of S is y. Then the first column of $S\Lambda$ is $\lambda_1 y$. If this is to agree with the first column of AS, which by matrix multiplication is Ay, then y must be an eigenvector: $Ay = \lambda_1 y$.

   (Note that the *order* of the eigenvectors in S and the eigenvalues in Λ must match.)

4. Not all matrices posses n linearly independent eigenvectors, so **not all matrices are diagonalizable**.

   Diagonalizability of A depends on having enough (n) independent eigenvectors. Invertibility of A depends on having nonzero eigenvalues.

   There is no connection between diagonalizability (n independent eigenvectors) and invertibility (no zero eigenvalues). The only indication given by the eigenvalues is that diagonalization can fail only if there are repeated eigenvalues. (But even then, it does not always fail–e.g. I.)

   The test is to check, for an eigenvalue that is repeated p times, whether there are p independent eigenvectors–in other words, whether $A - \lambda$ has rank $n - p$.

5. **Projection matrices always contain n independent eigenvectors and thus are always diagonalizable**.

Eigenvalues of Symmetric Matrices: If A is symmetric, then it has the following properties:

1. A has exactly n (not necessarily distinct) eigenvalues
2. There exists a set of n eigenvectors, one for each eigenvalue, that are mutually orthogonal (even if the eigenvalues are not distinct).

Eigenvalues of the Inverse of a Matrix: Suppose A is a square nonsingular matrix and λ is an eigenvalue of A. Then λ^{-1} is an eigenvalue of the matrix A^{-1}. Proof: Note that since A is nonsingular, A^{-1} exists and λ is nonnegative for all eigenvalues of A. Let λ be an eigenvalue of A and let $x \neq 0$ be an eigenvector of A for λ. Suppose A is n by n. Then we have

$$A^{-1}x = A^{-1}\lambda^{-1}\lambda x = \lambda^{-1}A^{-1}\lambda x = \lambda^{-1}A^{-1}Ax = \lambda^{-1}x$$

The inverse of a symmetric matrix is symmetric. Proof: Let A be a symmetric matrix.

$$I = I'$$

$$AA^{-1} = (AA^{-1})'$$

$$A^{-1}A = (A^{-1})'A'$$

$$A^{-1}AA^{-1} = (A^{-1})'AA^{-1}$$

$$A^{-1} = (A^{-1})'$$

Positive Definite Matrices

For any real invertible matrix A, the product $A'A$ is a positive definite matrix. (Proof: Let z be a non-zero vector. We want $z'A'Az > 0 \forall z$. Note that $z'A'Az = (Az)'(Az)$. Because A is invertible and $z \neq 0$, $Az \neq 0$, so $(Az)'(Az) > 0$.)

Let $A \in \mathbb{R}^{m \times n}$ with $m \geq n$ and let $\text{rank}(A) = n$ (that is, A has full column rank). Then $A'A$ is a positive definite matrix. (Proof: Let z be a non-zero vector. We want $z'A'Az > 0 \forall z$. Note that $z'A'Az = (Az)'(Az)$. Because A has full column rank (and n linearly independent columns) and $z \neq 0$, $Az \neq 0$, so $(Az)'(Az) > 0$.)

Every positive definite matrix is invertible and its inverse is also positive definite.

Practice Problems

12. Let A be a 2×2 matrix for which there is a constant k such that the sum of the entries in each row and each column is k. Which of the following must be an eigenvector of A ?

I. $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

II. $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

III. $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

(A) I only (B) II only (C) III only (D) I and II only (E) I, II, and III

Solution 12. (C) This condition makes the matrix of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

There is no reason that $a = 0$ or $b = 0$, so there is no reason $(1, 0)$ or $(0, 1)$ should be eigenvectors. But it is easy to verify that $(1, 1)$ must be.

24. Consider the system of linear equations

$$\begin{aligned} w + 3x + 2y + 2z &= 0 \\ w + 4x + y &= 0 \\ 3w + 5x + 10y + 14z &= 0 \\ 2w + 5x + 5y + 6z &= 0 \end{aligned}$$

with solutions of the form (w, x, y, z), where w, x, y, and z are real. Which of the following statements is FALSE?

(A) The system is consistent.

(B) The system has infinitely many solutions.

(C) The sum of any two solutions is a solution.

(D) $(-5, 1, 1, 0)$ is a solution.

(E) Every solution is a scalar multiple of $(-5, 1, 1, 0)$.

Solution 24. (E) Looking at our answers, we can verify directly that $(-5, 1, 1, 0)$ is a solution. Any multiple of $(-5, 1, 1, 0)$ is also a solution, which shows that (A), (B), (C), and (D) are all true – leaving only (E). Another solution, for example, is $(0, 2, -8, 5)$

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 3 & 4 & 5 \\ 0 & 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

34. Which of the following statements about the real matrix shown above is FALSE?

(A) A is invertible.

(B) If $\mathbf{x} \in \mathbb{R}^5$ and $A\mathbf{x} = \mathbf{x}$, then $\mathbf{x} = \mathbf{0}$.

(C) The last row of A^2 is $(0 \quad 0 \quad 0 \quad 0 \quad 25)$.

(D) A can be transformed into the 5×5 identity matrix by a sequence of elementary row operations.

(E) $\det(A) = 120$

Solution 34. (B) An upper triangular matrix is easily verified to be invertible so long as its diagonal entries are all nonzero. Specifically, $\det A$ is still the product of its diagonal entries, so (E) and (D) and (A) are all true. (C) can easily be verified to be true by computing that the bottom-right corner is 25 (the product of upper triangular matrices still being upper triangular). This leaves (B). (B) can be checked directly to be false: if we let $x = (1, 0, 0, 0, 0)$, then $Ax = x$.

37. Let V be a finite-dimensional real vector space and let P be a linear transformation of V such that $P^2 = P$. Which of the following must be true?

I. P is invertible.

II. P is diagonalizable.

III. P is either the identity transformation or the zero transformation.

(A) None (B) I only (C) II only (D) III only (E) II and III

Solution 37. (C) $P^2 = P$ means that P is projection onto some subspace. There is no reason to believe that this should be invertible, but it should definitely be diagonalisable (with eigenbasis some basis of that subspace). III also need not be true if the subspace is anything proper or nontrivial.

50. Let A be a real 2×2 matrix. Which of the following statements must be true?

I. All of the entries of A^2 are nonnegative.

II. The determinant of A^2 is nonnegative.

III. If A has two distinct eigenvalues, then A^2 has two distinct eigenvalues.

(A) I only (B) II only (C) III only (D) II and III only (E) I, II, and III

Solution 50. (B) There is no reason that all the entires of A^2 need to be nonnegative. Its determinant must be nonnegative though: $\det(A^2) = (\det A)^2$. For III, suppose A is the diagonal matrix with entires $\pm\lambda$. Then those are its eigenvalues, and they are distinct so long as $\lambda \neq 0$. But A^2 has only one eigenvalue: λ^2.

51. Which of the following is an orthonormal basis for the column space of the real matrix $\begin{pmatrix} 1 & -1 & 2 & -3 \\ -1 & 1 & -3 & 2 \\ 2 & -2 & 5 & -5 \end{pmatrix}$?

(A) $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$

(B) $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$

(C) $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \\ 0 \end{pmatrix} \right\}$

(D) $\left\{ \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix} \right\}$

(E) $\left\{ \begin{pmatrix} \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \\ \frac{2}{\sqrt{6}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \right\}$

Solution 51. (E) The basis (C) is not orthogonal and (D) is not normal, so we can rule those out. We can throw out the first column, since it is the negation of the second. A little bit of math shows that the remaining 3×3 matrix has determinant 0, so the rank of our column space is 2. That leaves only (A) and (E), but (A) cannot be correct. Our column space contains vectors that have nonzero third entry, so cannot lie in the span of that basis.

Calculus

List of common derivatives and integrals to know

$$\frac{d}{dx}\left(\sin^{-1}x\right)=\frac{1}{\sqrt{1-x^2}} \qquad \frac{d}{dx}\left(\ln\left(x\right)\right)=\frac{1}{x},\ x>0$$
$$\frac{d}{dx}\left(\cos^{-1}x\right)=-\frac{1}{\sqrt{1-x^2}} \qquad \frac{d}{dx}\left(\ln|x|\right)=\frac{1}{x},\ x\neq 0$$
$$\frac{d}{dx}\left(\tan^{-1}x\right)=\frac{1}{1+x^2} \qquad \frac{d}{dx}\left(\log_a\left(x\right)\right)=\frac{1}{x\ln a},\ x>0$$

$$\int \tan u\,du=\ln|\sec u|+c$$
$$\int \sec u\,du=\ln|\sec u+\tan u|+c$$
$$\int \tfrac{1}{a^2+u^2}\,du=\tfrac{1}{a}\tan^{-1}\left(\tfrac{u}{a}\right)+c$$
$$\int \tfrac{1}{\sqrt{a^2-u^2}}\,du=\sin^{-1}\left(\tfrac{u}{a}\right)+c$$

$$\int \ln u\,du=u\ln\left(u\right)-u+c$$

$\int \sinh x\,dx = \cosh x + C$ $\int \cosh x\,dx = \sinh x + C$

Optimizing functions of several variables

Functions of two variables [edit]

Suppose that $f(x, y)$ is a differentiable real function of two variables whose second partial derivatives exist. The Hessian matrix H of f is the 2×2 matrix of partial derivatives of f:

$$H(x,y)=\begin{pmatrix} f_{xx}(x,y) & f_{xy}(x,y) \\ f_{yx}(x,y) & f_{yy}(x,y) \end{pmatrix}.$$

Define $D(x, y)$ to be the determinant

$$D(x,y)=\det(H(x,y))=f_{xx}(x,y)f_{yy}(x,y)-\left(f_{xy}(x,y)\right)^2\ ,$$

of H. Finally, suppose that (a, b) is a critical point of f (that is, $f_x(a, b) = f_y(a, b) = 0$). Then the second partial derivative test asserts the following:[1]

1. If $D(a,b)>0$ and $f_{xx}(a,b)>0$ then (a,b) is a local minimum of f.
2. If $D(a,b)>0$ and $f_{xx}(a,b)<0$ then (a,b) is a local maximum of f.
3. If $D(a,b)<0$ then (a,b) is a saddle point of f.
4. If $D(a,b)=0$ then the second derivative test is inconclusive, and the point (a, b) could be any of a minimum, maximum or saddle point.

Functions of many variables [edit]

For a function *f* of two or more variables, there is a generalization of the rule above. In this context, instead of examining the determinant of the Hessian matrix, one must look at the eigenvalues of the Hessian matrix at the critical point. The following test can be applied at any critical point (*a*, *b*, ...) for which the Hessian matrix is invertible:

1. If the Hessian is positive definite (equivalently, has all eigenvalues positive) at (*a*, *b*, ...), then *f* attains a local minimum at (*a*, *b*, ...).
2. If the Hessian is negative definite (equivalently, has all eigenvalues negative) at (*a*, *b*, ...), then *f* attains a local maximum at (*a*, *b*, ...).
3. If the Hessian has both positive and negative eigenvalues then (*a*, *b*, ...) is a saddle point for *f* (and in fact this is true even if (*a*, *b*, ...) is degenerate).

Lagrange Multipliers

: to flesh out! http://tutorial.math.lamar.edu/Classes/CalcIII/LagrangeMultipliers.aspx

Line Integrals

(p. 555 of Strang book)

Suppose a force in two-dimensional space is given by $\boldsymbol{F} = M\boldsymbol{i} + N\boldsymbol{j}$. Then the work done by this force on a particle moving along a curve C is given by

$$W = \int_C \boldsymbol{F} \cdot \mathrm{d}\boldsymbol{R} = \int_C M\mathrm{d}x + N\mathrm{d}y$$

Along a curve in three-dimensional space the work done by a three-dimensional force $\boldsymbol{F} = M\boldsymbol{i} + N\boldsymbol{j} + P\boldsymbol{j}$ is given by

$$W = \int_C \boldsymbol{F} \cdot \boldsymbol{T}\mathrm{d}s = \int_C \boldsymbol{F} \cdot \mathrm{d}\boldsymbol{R} = \int_C M\mathrm{d}x + N\mathrm{d}y + P\mathrm{d}z$$

where the tangent vector $\boldsymbol{T}$ is given by

$$\boldsymbol{T} = \frac{\mathrm{d}\boldsymbol{R}}{\mathrm{d}s}$$

Green's Theorem: Suppose the region R is bounded by the simple closed piecewise smooth curve C. Then an integral over R equals a line integral around C:

$$\oint_C \boldsymbol{F} \cdot \mathrm{d}\boldsymbol{R} = \oint_C M\mathrm{d}x + N\mathrm{d}y = \int\int_R \left(\frac{\partial N}{\partial x} - \frac{\partial M}{\partial y}\right)\mathrm{d}x\ \mathrm{d}y$$

Miscellaneous

13A The tangent plane at (x_0, y_0, z_0) has the same slopes as the surface $z = f(x, y)$. The equation of the tangent plane (a linear equation) is

$$z - z_0 = \left(\frac{\partial f}{\partial x}\right)_0 (x - x_0) + \left(\frac{\partial f}{\partial y}\right)_0 (y - y_0). \tag{1}$$

The normal vector $\mathbf{N}$ to that plane has components $(\partial f/\partial x)_0$, $(\partial f/\partial y)_0$, -1.

13B The tangent plane to the surface $F(x, y, z) = c$ has the linear equation

$$\left(\frac{\partial F}{\partial x}\right)_0 (x - x_0) + \left(\frac{\partial F}{\partial y}\right)_0 (y - y_0) + \left(\frac{\partial F}{\partial z}\right)_0 (z - z_0) = 0. \tag{7}$$

The normal vector is $\mathbf{N} = \left(\frac{\partial F}{\partial x}\right)_0 \mathbf{i} + \left(\frac{\partial F}{\partial y}\right)_0 \mathbf{j} + \left(\frac{\partial F}{\partial z}\right)_0 \mathbf{k}$.

$$dz = (\partial z/\partial x)_0 dx + (\partial z/\partial y)_0 dy \quad \text{or} \quad df = f_x dx + f_y dy. \tag{10}$$

This is the ***total differential***. All letters dz and df and dw can be used, but ∂z and ∂f are not used. Differentials suggest small movements in x and y; then dz is the resulting movement in z. On the tangent plane, equation (10) holds exactly.

The **directional derivative**, denoted $D_v f(x, y)$, is a derivative of a multivariable function in the direction of a vector $\boldsymbol{v}$. It is the scalar projection of the gradient onto $\boldsymbol{v}$.

$$D_v f(x, y) = \text{comp}_v \nabla f(x, y) = \frac{\nabla f(x, y) \cdot \boldsymbol{v}}{|\boldsymbol{v}|}$$

Practice Problems

13F The directional derivative is $D_u f = (\text{grad } f) \cdot \mathbf{u}$. The level direction is perpendicular to grad f, since $D_u f = 0$. ***The slope $D_u f$ is largest when*** $\mathbf{u}$ ***is parallel to*** grad f. That maximum slope is the length $|\text{grad } f| = \sqrt{f_x^2 + f_y^2}$:

$$\textit{for} \quad \mathbf{u} = \frac{\text{grad } f}{|\text{grad } f|} \quad \textit{the slope is} \quad (\text{grad } f) \cdot \mathbf{u} = \frac{|\text{grad } f|^2}{|\text{grad } f|} = |\text{grad } f|.$$

$$\int_C g(x, y)\, ds = \text{limit of } \sum_{i=1}^{N} g(x_i, y_i) \Delta s_i \quad \text{as} \quad (\Delta s)_{\max} \to 0.$$

The differential ds ***becomes*** $(ds/dt)dt$. Everything changes over to t:

$$\int g(x, y)ds = \int_{t=a}^{t=b} g(x(t), y(t)) \sqrt{(dx/dt)^2 + (dy/dt)^2}\, dt.$$

19. Let f and g be twice-differentiable real-valued functions defined on $\mathbb{R}$. If $f'(x) > g'(x)$ for all $x > 0$, which of the following inequalities must be true for all $x > 0$?

(A) $f(x) > g(x)$

(B) $f''(x) > g''(x)$

(C) $f(x) - f(0) > g(x) - g(0)$

(D) $f'(x) - f'(0) > g'(x) - g'(0)$

(E) $f''(x) - f''(0) > g''(x) - g''(0)$

Solution 19. (C) There is no reason that $f(x) > g(x)$, or that $f''(x) > g''(x)$. But we do know that

$$\int_0^x f'(t)\, dt > \int_0^x g'(t)\, dt \implies f(x) - f(0) > g(x) - g(0).$$

This is precisely an answer.

22. What is the volume of the solid in xyz-space bounded by the surfaces $y = x^2$, $y = 2 - x^2$, $z = 0$, and $z = y + 3$?

(A) $\frac{8}{3}$ (B) $\frac{16}{3}$ (C) $\frac{32}{3}$ (D) $\frac{104}{105}$ (E) $\frac{208}{105}$

Solution 22. (C) It looks like our x-coordinates are running over $[-1, 1]$, with y depending on x and z depending on y. To find the volume of the solid, we just need to integrate the constant function 1. We must therefore compute

$$\begin{aligned}
\int_{-1}^{1}\int_{x^2}^{2-x^2}\int_{0}^{y+3} 1\, dz\, dy\, dx &= \int_{-1}^{1}\int_{x^2}^{2-x^2} y + 3\, dy\, dx \\
&= \int_{-1}^{1} \left((2-x^2)^2/2 + 3(2-x^2)\right) - \left((x^2)^2/2 + 3(x^2)\right) dx \\
&= \int_{-1}^{1} 8 - 8x^2\, dx \\
&= 8x - 8x^3/3\Big|_{-1}^{1} = (8 - 8/3) - (-8 + 8/3) = 32/3.
\end{aligned}$$

24. Let h be the function defined by $h(x) = \int_0^{x^2} e^{x+t}\, dt$ for all real numbers x. Then $h'(1) =$

(A) $e - 1$ (B) e^2 (C) $e^2 - e$ (D) $2e^2$ (E) $3e^2 - e$

Solution 24. (E) We can actually just integrate this, and not worry about differentiation under the integral.

$$\int_0^{x^2} e^{x+t}\,dt = e^x \int_0^{x^2} e^t\,dt = e^x(e^{x^2}-1) = e^{x^2+x} - e^x.$$

Then deriving that,

$$h'(x) = (2x+1)e^{x^2+x} - e^x,$$

whence our result follows immediately.

26. Let $f(x, y) = x^2 - 2xy + y^3$ for all real x and y. Which of the following is true?

(A) f has all of its relative extrema on the line $x = y$.

(B) f has all of its relative extrema on the parabola $x = y^2$.

(C) f has a relative minimum at $(0, 0)$.

(D) f has an absolute minimum at $\left(\frac{2}{3}, \frac{2}{3}\right)$.

(E) f has an absolute minimum at $(1, 1)$.

Solution 26. (A) We are concerned about its extrema, we should find some partial derivatives.

$$f_x = 2x - 2y, \quad f_y = -2x + 3y^2.$$

We would like to know when they are both zero. The first equation gives us $x = y$ and the second gives us $2x = 3y^2$, so that

$$2y = 3y^2 \implies (3y-2)y = 0 \implies y = 0, 2/3.$$

Therefore our solutions are $(0, 0)$ and $(2/3, 2/3)$. Indeed, our relative extrema are all on the line $x = y$. To do some more checking (which you should not do on the actual test),

$$f_{xx} = 2, \quad f_{yy} = 6y, \quad f_{xy} = f_{yx} = -2.$$

Then the determinant of the Hessian is $12y - 4$. This shows that $(0, 0)$ is a saddle point. There is no reason that $(2/3, 2/3)$ is an absolute minimum without further verification, and $(1, 1)$ needn't be an extreme point.

27. Consider the two planes $x + 3y - 2z = 7$ and $2x + y - 3z = 0$ in $\mathbb{R}^3$. Which of the following sets is the intersection of these planes?

(A) $\varnothing$

(B) $\{(0, 3, 1)\}$

(C) $\{(x, y, z) : x = t,\ y = 3t,\ z = 7 - 2t,\ t \in \mathbb{R}\}$

(D) $\{(x, y, z) : x = 7t,\ y = 3 + t,\ z = 1 + 5t,\ t \in \mathbb{R}\}$

(E) $\{(x, y, z) : x - 2y - z = -7\}$

Solution 27. (D) First, we know that the intersection of two planes in $\mathbb{R}^3$ should be either a plane or a line. In our case, the two planes are definitely not the same, so we will obtain a line. The slope of the line can be found by taking the cross product of the normal vectors of the two planes in question.

$$(1,3,-2) \times (2,1,-3) = \det \begin{bmatrix} i & j & k \\ 1 & 3 & -2 \\ 2 & 1 & -3 \end{bmatrix} = (-7,-1,-5).$$

The only solution corresponding to this slope is (D), as the coefficients of t in (x,y,z) are $(7,1,5)$.

32. $\frac{d}{dx}\int_{x^3}^{x^4} e^{t^2}\,dt =$

(A) $e^{x^6}\left(e^{x^8-x^6}-1\right)$ (B) $4x^3e^{x^8}$ (C) $\frac{1}{\sqrt{1-e^{x^2}}}$ (D) $\frac{e^{x^2}}{x^2}-1$ (E) $x^2e^{x^6}\left(4xe^{x^8-x^6}-3\right)$

Solution 32. (E) We can sort this out in two steps and apply the fundamental theorem to each.

$$\frac{d}{dx}\left(\int_{x^3}^{0} e^{t^2}\,dx + \int_{0}^{x^4} e^{t^2}\,dx\right)$$

For the first,

$$\frac{d}{dx}\int_{x^3}^{0} e^{t^2}\,dx = -\frac{d}{dx}\int_{0}^{x^3} e^{t^2}\,dx = -3x^2e^{x^6}$$

For the second,

$$\frac{d}{dx}\int_{0}^{x^4} e^{t^2}\,dx = 4x^3e^{x^8}.$$

All told, our integral is $x^2e^{x^6}(4xe^{x^8-x^6}-3)$.

41. Let ℓ be the line that is the intersection of the planes $x+y+z=3$ and $x-y+z=5$ in $\mathbb{R}^3$. An equation of the plane that contains $(0,0,0)$ and is perpendicular to ℓ is

(A) $x-z=0$

(B) $x+y+z=0$

(C) $x-y-z=0$

(D) $x+z=0$

(E) $x+y-z=0$

Solution 41. (A) The first plane is determined by the normal vector $(1,1,1)$, and the second determined by $(1,-1,1)$. Therefore the slope of ℓ is determined by a vector perpendicular to those, i.e. the cross product.

$$(1,1,1) \times (1,-1,1) = \det \begin{bmatrix} i & j & k \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix} = (2,0,-2).$$

41. Let C be the circle $x^2 + y^2 = 1$ oriented counterclockwise in the xy-plane. What is the value of the line integral $\oint_C (2x - y)\,dx + (x + 3y)\,dy$?

(A) 0 (B) 1 (C) $\frac{\pi}{2}$ (D) π (E) 2π

Solution 41. (E) This is a classic Green's theorem problem.

$$\oint_{\partial D} L\,dx + M\,dy = \iint_D \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right) dx\,dy.$$

In our case,

$$\oint_C (2x - y)\,dx + (x + 3y)\,dy = \iint_D (1 + 1)\,dx\,dy = 2A,$$

where A is the area of the unit circle, i.e. π.

So that is the slope of ℓ. We need this to be the normal vector for the plane in question, so it seems that $(1,0,-1)$ is our best bet (out of the given options).

$$\begin{aligned} y' + xy &= x \\ y(0) &= -1 \end{aligned}$$

44. If y is a real-valued function defined on the real line and satisfying the initial value problem above, then $\lim_{x \to -\infty} y(x) =$

(A) 0 (B) 1 (C) -1 (D) ∞ (E) $-\infty$

Solution 44. (B) Putting it in simpler terms,

$$\frac{dy}{dx} + xy = x \implies \frac{dy}{dx} = x(1 - y) \implies \frac{dy}{1 - y} = x\,dx.$$

Integrating both sides, we obtain

$$-\log(1 - y) = x^2/2 + C' \implies 1 - y = Ce^{-x^2/2} \implies y = 1 - Ce^{-x^2/2}.$$

Solving the initial value problem gives $C = 2$. Furthermore, as $x \to -\infty$, the second term above vanishes so we get 1 in the limit.

48. Let g be the function defined by $g(x, y, z) = 3x^2y + z$ for all real x, y, and z. Which of the following is the best approximation of the directional derivative of g at the point $(0, 0, \pi)$ in the direction of the vector $\mathbf{i} + 2\mathbf{j} + 3\mathbf{k}$? (Note: $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ are the standard basis vectors in $\mathbb{R}^3$.)

(A) 0.2 (B) 0.8 (C) 1.4 (D) 2.0 (E) 2.6

Solution 48. (B) It would be good to recall the formula for the directional derivative. We take the gradient of the function then take its scalar product with the normalised vector in the direction we want. To begin,

$$\nabla g = (6xy, 3x^2, 1).$$

At the point $(0, 0, \pi)$, we have $\nabla g = (0, 0, 1)$. That works out pretty well for us. The normalised version of the vector $(1, 2, 3)$ is $(1/\sqrt{14}, 2/\sqrt{14}, 3/\sqrt{14})$. Dotting this with $(0, 0, 1)$ gives $3/\sqrt{14}$, and since $\sqrt{14} = 3.5$ or so our answer should be closer to 0.8 than 0.2.

48. Consider the theorem: If f and f' are both strictly increasing real-valued functions on the interval $(0, \infty)$, then $\lim_{x\to\infty} f(x) = \infty$. The following argument is suggested as a proof of this theorem.

(1) By the Mean Value Theorem, there is a c_1 in the interval $(1, 2)$ such that

$$f'(c_1) = \frac{f(2) - f(1)}{2 - 1} = f(2) - f(1) > 0.$$

(2) For each $x > 2$, there is a c_x in $(2, x)$ such that $\dfrac{f(x) - f(2)}{x - 2} = f'(c_x)$.

(3) For each $x > 2$, $\dfrac{f(x) - f(2)}{x - 2} = f'(c_x) > f'(c_1)$ since f' is strictly increasing.

(4) For each $x > 2$, $f(x) > f(2) + (x - 2)f'(c_1)$.

(5) $\lim_{x\to\infty} f(x) = \infty$

Which of the following statements is true?

(A) The argument is valid.

(B) The argument is not valid since the hypotheses of the Mean Value Theorem are not satisfied in (1) and (2).

(C) The argument is not valid since (3) is not valid.

(D) The argument is not valid since (4) cannot be deduced from the previous steps.

(E) The argument is not valid since (4) does not imply (5).

Solution 48. (A) The only issue here seems to be that (4) implies that $f(x)$ gets very large so long as $f'(c_1)$ is positive. But we know that it is, since f is a strictly increasing function. Therefore everything is satisfactory.

Line integrals chapter! http://tutorial.math.lamar.edu/Classes/CalcIII/LineIntegralsIntro.aspx

Surface inegrals chapter! http://tutorial.math.lamar.edu/Classes/CalcIII/SurfaceIntegralsIntro.aspx

Differential Equations

61. A tank initially contains a salt solution of 3 grams of salt dissolved in 100 liters of water. A salt solution containing 0.02 grams of salt per liter of water is sprayed into the tank at a rate of 4 liters per minute. The sprayed solution is continually mixed with the salt solution in the tank, and the mixture flows out of the tank at a rate of 4 liters per minute. If the mixing is instantaneous, how many grams of salt are in the tank after 100 minutes have elapsed?

(A) 2 (B) $2 - e^{-2}$ (C) $2 + e^{-2}$ (D) $2 - e^{-4}$ (E) $2 + e^{-4}$

Solution 61. (E) We can set this up as a differential equation. Let s denote the amount of salt in the tank, and let t denote time. We have the initial condition of $s(0) = 3$. $s'(t)$ depends on two factors: the salt flowing in and the salt flowing out. The salt flows in constantly at a rate of 0.08 grams per minute, and the salt flows out at a rate of $4 \cdot (s/100) = s/25$ grams per minute. Therefore

$$s'(t) = \frac{ds}{dt} = 0.08 - s(t)/25 \implies \frac{ds}{dt} = 0.04(2 - s) \implies \frac{ds}{2 - s} = 0.04\, dt.$$

Doing the usual calculus,

$$-\log(2 - s) = 0.04t + C' \implies 2 - s = Ce^{-0.04t} \implies s(t) = 2 - Ce^{-0.04t}.$$

The initial condition tells us that $C = -1$, so $s(t) = 2 + e^{-0.04t}$. Plugging in $t = 100$ gives our answer.

Real Analysis

Brush up on recent real analysis (especially open, closed, compact, etc)

38. Let A and B be nonempty subsets of $\mathbb{R}$ and let $f : A \to B$ be a function. If $C \subseteq A$ and $D \subseteq B$, which of the following must be true?

(A) $C \subseteq f^{-1}\big(f(C)\big)$

(B) $D \subseteq f\big(f^{-1}(D)\big)$

(C) $f^{-1}\big(f(C)\big) \subseteq C$

Solution 38. (A) Neither of the equalities should hold – these are in fact nonsense statements, as one side lies in A and the other in B. To unravel the remaining two sets,

$$f^{-1}(f(C)) = \{x \in A : f(x) \in f(C)\}, \quad f(f^{-1}(D)) = f\left(\{y \in A : f(y) \in D\}\right)$$

Clearly the second set must always be contained in D, but not the other way around. Similarly the first set certainly contains all $c \in C$ (as $f(c) \in f(C)$) but not the other way around.

47. The function $f : \mathbb{R} \to \mathbb{R}$ is defined as follows.

$$f(x) = \begin{cases} 3x^2 & \text{if } x \in \mathbb{Q} \\ -5x^2 & \text{if } x \notin \mathbb{Q} \end{cases}$$

Which of the following is true?

(A) f is discontinuous at all $x \in \mathbb{R}$.

(B) f is continuous only at $x = 0$ and differentiable only at $x = 0$.

(C) f is continuous only at $x = 0$ and nondifferentiable at all $x \in \mathbb{R}$.

(D) f is continuous at all $x \in \mathbb{Q}$ and nondifferentiable at all $x \in \mathbb{R}$.

(E) f is continuous at all $x \notin \mathbb{Q}$ and nondifferentiable at all $x \in \mathbb{R}$.

Solution 47. (B) A classic kind of problem. We are clearly continuous and differentiable at 0. Anywhere else, near a rational number there is an irrational number and vice versa. Therefore there can be no continuity anywhere but at 0, and hence no differentiability either.

57. For each positive integer n, let x_n be a real number in the open interval $\left(0, \frac{1}{n}\right)$. Which of the following statements must be true?

I. $\lim_{n\to\infty} x_n = 0$

II. If f is a continuous real-valued function defined on $(0, 1)$, then $\{f(x_n)\}_{n=1}^{\infty}$ is a Cauchy sequence.

III. If g is a uniformly continuous real-valued function defined on $(0, 1)$, then $\lim_{n\to\infty} g(x_n)$ exists.

(A) I only (B) I and II only (C) I and III only (D) II and III only (E) I, II, and III

Solution 57. (C) I is true, since $\lim_{n\to\infty} x_n$ must be bounded between 0 and $\lim_{n\to\infty} 1/n = 0$. Unfortunately, x_n does not converge inside $(0, 1)$. There is no reason therefore that $f(x_n)$ should be a convergent sequence – suppose that $f(x) = 1/x$, so that $f(x_n)$ is certainly not Cauchy. However, if g is uniformly continuous, then g extends to a continuous function on $[0, 1]$. Now x_n is a convergent sequence, so $\lim_{n\to\infty} g(x_n) = g(\lim_{n\to\infty} x_n) = g(0)$ exists.

60. A real-valued function f defined on $\mathbb{R}$ has the following property.

For every positive number ϵ, there exists a positive number δ such that
$|f(x) - f(1)| \geq \epsilon$ whenever $|x - 1| \geq \delta$.

This property is equivalent to which of the following statements about f?

(A) f is continuous at $x = 1$.

(B) f is discontinuous at $x = 1$.

(C) f is unbounded.

(D) $\lim_{|x|\to\infty} |f(x)| = \infty$

(E) $\int_0^{\infty} |f(x)|dx = \infty$

Solution 60. (D) While it looks like this is the opposite of continuity, that should read 'there exists $\varepsilon > 0$'. What the statement says is that we not only get arbitrarily far away from $f(1)$, but we must for all x sufficiently far away from 1. So as $|x|$ gets very large, so does $|f(x)|$.

63. For any nonempty sets A and B of real numbers, let $A \cdot B$ be the set defined by

$$A \cdot B = \{xy : x \in A \text{ and } y \in B\}.$$

If A and B are nonempty bounded sets of real numbers and if $\sup(A) > \sup(B)$, then $\sup(A \cdot B) =$

(A) $\sup(A)\sup(B)$

(B) $\sup(A)\inf(B)$

(C) $\max\{\sup(A)\sup(B),\ \inf(A)\inf(B)\}$

(D) $\max\{\sup(A)\sup(B),\ \sup(A)\inf(B)\}$

(E) $\max\{\sup(A)\sup(B),\ \inf(A)\sup(B),\ \inf(A)\inf(B)\}$

Solution 63. (E) The supremum is either going to be the product of the two largest positive numbers in A and B or the product of the two smallest negative numbers in A and B. That means we should look for $\sup \cdot \sup$ or $\inf \cdot \inf$. However, it might be the case that B contains only negative numbers and A contains only positive numbers. Then the largest value in $A \cdot B$ will be attained by the smallest positive element of A and the largest negative element of B, giving us our third option: $\inf A \cdot \sup B$.

Probability

To Know for Math 505A Midterm 1 (Discrete Random Variables)

Definitions

A **probability mass function** of a discrete random variable

A **cumulative distribution function** or **distribution** of a discrete random variable

Two random variables are **uncorrelated** if and only if

Two random variables are **independent** if and only if

Discrete Random Variable Distributions

Binomial: mass function, distribution, expectation, variance, how to derive

Poisson: mass function, distribution, expectation, variance, how to derive

Geometric: mass function, expectation, variance; maybe: distribution, how to derive

Negative binomial: mass function, expectation; maybe: variance, distribution, how to derive

Hypergeometric: mass function, expectation; maybe: variance, distribution, how to derive

Indicator Method

Example problems: 505A Homework 3 problem 9(a)

Linear transformations of random variables

Poisson Paradigm (Poisson approximation for indicator method)

Asymptotic Distributions

$$e^x = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n$$

Stirling's Formula (double check):

$$\lim_{n\to\infty} n! \approx n^n e^{-n}\sqrt{2\pi n}$$

To Know for Math 505A Midterm 2

Definitions

A **probability density function** for a continuous random variable

A **cumulative distribution function** or **distribution** of a continuous random variable

Inequalities

Abstract Algebra

These are my notes from reading *Elementary Abstract Algebra* by W. Edwin Clark, available for free download on his website: http://shell.cas.usf.edu/~wclark/#ELEMENTARY_ABSTRACT_ALGEBRA

Chapter 1: Binary Operations

Definition 1.1 *A* **binary operation** $*$ *on a set* S *is a function from* $S \times S$ *to* S*. If* $(a, b) \in S \times S$ *then we write* $a * b$ *to indicate the image of the element* (a, b) *under the function* $*$*.*

The following lemma explains in more detail exactly what this definition means.

Lemma 1.1 *A binary operation* $*$ *on a set* S *is a rule for combining two elements of* S *to produce a third element of* S*. This rule must satisfy the following conditions:*

(a) $a \in S$ *and* $b \in S \implies a * b \in S$. [$S$ is closed under $*$.]

(b) *For all* a, b, c, d *in* S
$a = c$ *and* $b = d \implies a * b = c * d$. [Substitution is permissible.]

(c) *For all* a, b, c, d *in* S
$a = b \implies a * c = b * c$.

(d) *For all* a, b, c, d *in* S
$c = d \implies a * c = a * d$.

Definition: A **function** f from the set A to the set B is a rule which assigns to each element $a \in A$ an element $f(a) \in B$ in such a way that the following condition holds for all $x, y \in A$:

$$x = y \implies f(x) = f(y)$$

To indicate that f is a function from A to B we write $f : A \to B$. The set A is called the **domain** of f and the set B is called the **codomain** of f.

A function $f : A \to B$ is said to be **one-to-one** or **injective** if the following condition holds for all $x, y \in A$:

$$f(x) = f(y) \implies x = y$$

A function $f : A \to B$ is said to be **onto** or **surjective** if the following condition holds:

$$\forall\, b \in B\ \exists\, a \in A \mid f(a) = b$$

A function $f : A \to B$ is said to be **bijective** if it is both one-to-one and onto. Then f is sometimes said to be a **bijection** or a **one-to-one correspondence** between A and B.

15. Let S, T, and U be nonempty sets, and let $f : S \to T$ and $g : T \to U$ be functions such that the function $g \circ f : S \to U$ is one-to-one (injective). Which of the following must be true?

(A) f is one-to-one.

(B) f is onto.

(C) g is one-to-one.

(D) g is onto.

(E) $g \circ f$ is onto.

Solution 15. (A) For a composition of functions, if the first function isn't one-to-one, there's no way the composite is. It's worth mentioning here that the opposite is true for onto: the second function had better be onto.

Let S be a set. The **power set** $\mathcal{P}(S)$ of S is the set of all subsets of S (including S itself).

Definition 1.2 *Assume that $*$ is a binary operation on the set S.*

1. *We say that $*$ is* **associative** *if*

$$x * (y * z) = (x * y) * z \quad \text{for all } x, y, z \in S.$$

2. *We say that an element e in S is an* **identity** *with respect to $*$ if*

$$x * e = x \text{ and } e * x = x \quad \text{for all } x \text{ in } S.$$

3. *Let $e \in S$ be an identity with respect to $*$. Given $x \in S$ we say that an element $y \in S$ is an* **inverse** *of x if both*

$$x * y = e \text{ and } y * x = e.$$

4. *We say that $*$ is* **commutative** *if*

$$x * y = y * x \quad \text{for all } x, y \in S.$$

5. *We say that an element a of S is* **idempotent** *with respect to $*$ if*

$$a * a = a.$$

6. *We say that an element z of S is a* **zero** *with respect to $*$ if*

$$z * x = z \text{ and } x * z = z \quad \text{for all } x \in S.$$

For each integer $n \geq 2$ define the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

For all $a, b \in \mathbb{Z}_n$ let

$$a + b = \text{remainder when the ordinary sum of a and b is divided by n}$$

and

$$a \cdot b = \text{remainder when the ordinary product of a and b is divided by n.}$$

These binary operations are referred to as **addition modulo** n and **multiplication modulo** n. The integer n in $\mathbb{Z}_n$ is called the **modulus**. The plural of modulus is **moduli**.

Let K denote any one of the following: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$.

$$M_n(K)$$

is the set of all $n \times n$ matrices containing elements of K.

$$GL(n, K)$$

is the set of all matrices in $M_n(K)$ with non-zero determinant. $(GL(n, k), \cdot)$ is called the **general linear group of degree n over K**. It is non-abelian.

$$SL(n, K) = \{A \in GL(n, K) \mid \det(A) = 1\}$$

$SL(n, K)$ is called the **Special Linear Group of degree** n **over** K.

Chapter 2: Groups

Definition A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following properties:

1. **The binary operation is associative on G:** $\forall\ x, y, z \in G$,

$$x * (y * z) = (x * y) * z$$

2. **The binary operation contains a (unique) identity in G:** $\exists\ e \in G \mid \forall\ x \in G$

$$e * x = x,\ x * e = x$$

3. **Every element in G has a (unique) inverse on $*$ in G:** $\forall\ x \in G\ \exists\ y \in G \mid$

$$x * y = e, y * x = e$$

A group $(G, *)$ is said to be **abelian** if $\forall\ x, y \in G,\ x * y = y * x$. A group is said to be **non-abelian** if it is not abelian.

Theorem 2.2 *Let $(G, *)$ be a group with identity e. Then the following hold for all elements a, b, c, d in G:*

1. *If $a * c = a * b$, then $c = b$.* [Left cancellation law for groups.]
2. *If $c * a = b * a$, then $c = b$.* [Right cancellation law for groups.]
3. *Given a and b in G there is a* unique *element x in G such that $a * x = b$.*
4. *Given a and b in G there is a* unique *element x in G such that $x * a = b$.*
5. *If $a * b = e$ then $a = b^{-1}$ and $b = a^{-1}$.* [Characterization of the inverse of an element.]
6. *If $a * b = a$ for just one a, then $b = e$.*
7. *If $b * a = a$ for just one a, then $b = e$.*
8. *If $a * a = a$, then $a = e$.* [The only idempotent in a group is the identity.]
9. $(a^{-1})^{-1} = a$.
10. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Chapter 3: The Symmetric Groups

If n is a positive integer,

$$[n] = \{1, 2, \ldots, n\}$$

A **permutation** of $[n]$ is a one-to-one, onto function from $[n]$ to $[n]$, and

$$S_n$$

is the set of all permutations of $[n]$.

The identity of S_n is the so-called **identity function**

$$\iota : [n] \to [n]$$

which is defined by the rule

$$\iota(x) = x, \quad \forall\ x \in [n]$$

The inverse of an element $\sigma \in S_n$: Suppose $\sigma \in S_n$. Since σ is by definition one-to-one and onto, the rule

$$\sigma^{-1}(y) = x \iff \sigma(x) = y$$

defines a function $\sigma^{-1} : [n] \to [n]$. This function σ^{-1} is also one-to-one and onto and satisfies

$$\sigma\sigma^{-1} = \iota \text{ and } \sigma^{-1}\sigma = \iota$$

so it is the inverse of σ in the group sense also.

Since the binary operation of composition on S_n is associative $[(\gamma\beta)\alpha = \gamma(\beta\alpha)]$, S_n under the binary operation of composition is a group (it is associative, it has an inverse, and it has an identity).

Definition 3.2 *Let $i_1, i_2, \ldots, i_k$ be a list of k distinct elements from $[n]$. Define a permuation σ in S_n as follows:*

$$\begin{aligned} \sigma(i_1) &= i_2 \\ \sigma(i_2) &= i_3 \\ \sigma(i_3) &= i_4 \\ \vdots &\ \vdots\ \ \vdots \\ \sigma(i_{k-1}) &= i_k \\ \sigma(i_k) &= i_1 \end{aligned}$$

and if $x \notin \{i_1, i_2, \ldots, i_k\}$ then

$$\sigma(x) = x$$

Such a permutation is called a **cycle** *or a k-***cycle** *and is denoted by*

$$(i_1\ i_2\ \cdots\ i_k).$$

If $k = 1$ then the cycle $\sigma = (i_1)$ is just the identity function, i.e., $\sigma = \iota$.

Two cycles $(i_1\ i_2\ \ldots\ i_k)$ and $(j_1\ j_2\ \ldots\ j_l)$ are said to be **disjoint** if the sets $\{i_1, i_2, \ldots, i_k\}$ and $\{j_1, j_2, \ldots, j_l\}$ are disjoint.

So for example, the cycles (1 2 3) and (4 5 8) are disjoint, but the cycles (1 2 3) and (4 2 8) are not disjoint.

If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

Theorem 3.4 *Every element $\sigma \in S_n$, $n \geq 2$, can be written as a product*

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m \tag{3.1}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_m$ are pairwise disjoint cycles, that is, for $i \neq j$, σ_i and σ_j are disjoint. If all 1-cycles of σ are included, the factors are unique except for the order. ■

The factorization (3.1) is called the **disjoint cycle decomposition of** σ.

An element of S_n is called a **transposition** if and only if it is a 2-cycle.

Every element of S_n can be written as a product of transpositions. The factors of such a product are not unique. However, if $\sigma \in S_n$ can be written as a product of k transpositions and if the same σ can also be written as a product of l transpositions, then k and l have the same parity.

A permutation is **even** if it is a product of an even number of transpositions and **odd** if it is a product of an odd number of transpositions. We define the function sign : $S_n \to \{1, -1\}$ by

$$\text{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

If $n = 1$ then there are no transpositions. In this case, to be complete we define the identity permutation ι to be even.

If σ is a k-cycle, then $\text{sign}(\sigma) = 1$ if k is odd and $\text{sign}(\sigma) = -1$ if k is even.

Remark. Let $A = [a_{ij}]$ be an $n \times n$ matrix. The determinant of A may be defined by the sum

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

For example, if $n = 2$ we have only two permutations ι and $(1\ 2)$. Since $\text{sign}(\iota) = 1$ and $\text{sign}((1\ 2)) = -1$ we obtain

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Definition: If $(G, *)$ is a group, the number of elements in G is called the **order** of G. We use $|G|$ to denote the order of G. Note that $|G|$ may be finite or infinite.

Let

$$A_n$$

be the set of all even permutations in the group S_n. A_n is called the **alternating group of degree** n.

Chapter 4: Subgroups

Definition: Let G be a group. A **subgroup** of G is a subset H of G which satisfies the following three conditions:

1. $e \in H$
2. $a, b \in H \implies ab \in H$
3. $a \in H \implies a^{-1} \in H$

If H is a subgroup of G, we write $H \leq G$. The subgroups $\{e\}$ and G are said to be **trivial** subgroups of G.

Every finite subgroup may be thought of as a subgroup of one of the groups S_n.

Let A_n be the set of all even permutations in the group S_n. A_n is then a subgroup of S_n. A_n is called the **alternating group of degree** n.

Let a be an element of the group G. If $\exists\ n \in \mathbb{N} \mid a^n = e$ we say that a has **finite order** and we define

$$\mathrm{o}(a) = \min\{n \in \mathbb{N} \mid a^n = e\}$$

If $a^n \neq e\ \forall\ n \in \mathbb{N}$ we say that a has **infinite order** and we define

$$\mathrm{o}(a) = \infty$$

In either case we call $\mathrm{o}(a)$ the **order** of a. Note carefully the difference between the order of a group and the order of an element of a group. Note also that $a = e \iff \mathrm{o}(a) = 1$. So every element of a group other than e has order $n \geq 2$ or ∞.

Let a be an element of group G. Define

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

We call $\langle a \rangle$ the **subgroup of G generated by** a. Note that $e = a^0$ and a^{-1} are in $\langle a \rangle$.

Theorem. For each $a \in G$, $\langle a \rangle$ is a subgroup of G. $\langle a \rangle$ contains a and is the smallest subgroup of G containing a.

Proof of second statement. If H is any subgroup of G containing a, $\langle a \rangle \subseteq H$ since H is closed under taking products and inverses. That is, every subgroup of G containing a also contains $\langle a \rangle$. This implies that $\langle a \rangle$ is the smallest subgroup of G containing a.

Theorem. Let G be a group and let $a \in G$. If $o(a) = 1$, then $\langle a \rangle = \{e\}$. If $o(a) = n$ where $n \geq 2$, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and the elements $e, a, a^2, \ldots, a^{n-1}$ are distinct; that is,

$$o(a) = |\langle a \rangle|$$

Proof Assume that $o(a) = n$. The case $n = 1$ is left to the reader. Suppose $n \geq 2$. We must prove two things.

1. If $i \in \mathbb{Z}$ then $a^i \in \{e, a, a^2, \ldots, a^{n-1}\}$.
2. The elements $e, a, a^2, \ldots, a^{n-1}$ are distinct.

To establish 1 we note that if i is any integer we can write it in the form $i = nq + r$ where $r \in \{0, 1, \ldots, n-1\}$. Here q is the quotient and r is the remainder when i is divided by n. Now using Theorem 2.4 we have

$$a^i = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

This proves 1. To prove 2, assume that $a^i = a^j$ where $0 \leq i < j \leq n-1$. It follows that

$$a^{j-i} = a^{j+(-i)} = a^j a^{-i} = a^i a^{-i} = a^0 = e.$$

But $j - i$ is a positive integer less than n, so $a^{j-i} = e$ contradicts the fact that $o(a) = n$. So the assumption that $a^i = a^j$ where $0 \leq i < j \leq n-1$ is false. This implies that 2 holds. It follows that $\langle a \rangle$ contains exactly n elements, that is, $o(a) = |\langle a \rangle|$.

Theorem. If G is a finite group, then every element of G has finite order.

49. What is the largest order of an element in the group of permutations of 5 objects?

(A) 5 (B) 6 (C) 12 (D) 15 (E) 120

Solution 49. (B) The greatest order is given by the product of a 2-cycle and a 3-cycle acting on disjoint elements. That gives order 6.

Chapter 5: The Group of Units of $\mathbb{Z}_n$

Let $n \geq 2$. An element $a \in \mathbb{Z}_n$ is said to be a **unit** if $\exists\ b \in \mathbb{Z}_n \mid ab = 1$ (where the product is multiplication modulo n).

The set of all units in $\mathbb{Z}_n$ is denoted by

$$U_n$$

and is a group under multiplication modulo n called the **group of units of** $\mathbb{Z}_n$.

Theorem. For $n \geq 2$, $U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$

Theorem. p is a prime $\implies \exists\ a \in U_p \mid U_p = \langle a \rangle$

Theorem. If $n \geq 2$ then U_n contains an element a satisfying $U_n = \langle a \rangle$ if and only if a has one of the following forms: $2,\ 4,\ p^k$, or $2p^k$ where p is an odd prime and $k \in \mathbb{N}$.

Chapter 6: Direct Products of Groups

If $G_1, G_2, \ldots, G_n$ is a list of n groups we make the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ into a group by defining the binary operation

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

Here for each $i \in \{1, 2, \ldots, n\}$ the product $a_i \cdot b_i$ is the product of a_i and b_i in the group G_i. We call this group the **direct product** of the groups $G_1, G_2, \ldots, G_n$.

The direct product contains an identity and an inverse, and is associative (since it is composed of groups which must themselves be associative), so it is a group per below:

Theorem. If $G_1, G_2, \ldots, G_n$ is a list of n groups, the direct product $G = G_1 \times G_2 \times \cdots \times G_n$ as defined above is a group. Moreover, if for each i, e_i is the identity of G_i, then $e_1, e_2, \ldots, e_n$ is the identity of G, and if

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in G$$

then the inverse of $\boldsymbol{a}$ is given by

$$\boldsymbol{a}^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$$

where a_i^{-1} is the inverse of a_i in the group G_i.

Chapter 7: Isomorphism of Groups

Let $G = \{g_1, g_2, \ldots, g_n\}$. Let $o(g_i) = k_i$ for $i = 1, 2, \ldots, n$. We say that the sequence $(k_1, k_2, \ldots, k_m)$ is the **order sequence** of the group G. To make the sequence unique we assume the elements are ordered so that $k_1 \leq k_2 \leq \ldots \leq k_n$.

Let $(G, *)$ and $(H, \bullet)$ be groups. A function $f : G \to H$ is said to be a **homomorphism** from G to H if

$$f(a * b) = f(a) \bullet f(b)$$

for all $a, b \in G$. If in addition f is one-to-one and onto, f is said to be an **isomorphism** from G to H.

We say that G and H are **isomorphic** if and only if there is an isomorphism from G to H. We write $G \cong H$ to indicate that G is isomorphic to H.

Isomorphism is an equivalence relation: If G, H, and K are groups then

1. $G \cong G$
2. If $G \cong H$ then $H \cong G$, and
3. If $G \cong H$ and $H \cong K$, then $G \cong K$.

Theorem. Let $(G, *)$ and $(H, \bullet)$ be groups and let $f : G \to H$ be a homomorphism. Let e_G denote the identity of G, and let e_H denote the identity of H. Then

1. $f(e_G) = e_H$

Proof: Let $x_G \in G$ and let $f(x_G) = x_H \in H$. Then
$x_H = f(x_G) = f(e_G * x_G) = f(e_G) \bullet f(x_G) = f(e_G) \bullet x_H = e_H \bullet x_H$.

2. $f(a^{-1}) = f(a)^{-1}$

Proof: $f(a)^{-1} \bullet f(a) = e_H = f(e_G) = f(a^{-1} * a) = f(a^{-1}) \bullet f(a)$

3. $f(a^n) = f(a)^n \ \forall \ n \in \mathbb{Z}$

Proof by induction.

Theorem. Let $(G, *)$ and $(H, \bullet)$ be groups and let $f : G \to H$ be an isomorphism. Then $o(a) = o(f(a)) \ \forall \ a \in G$. It follows that G and H have the same number of elements of each possible order.

Theorem. If G and H are isomorphic groups, and G is abelian, then so is H.

Proof: Let $a_G, b_G \in G$ and let $f(a_G) = a_H \in H, f(b_G) = b_H \in H$.
$a_H \bullet b_H = f(a_G) \bullet f(b_G) = f(a_G * b_G) = f(b_G * a_G) = f(b_G) \bullet f(a_G) = b_H \bullet a_H$.

A group G is **cyclic** if there is an element $a \in G \mid \langle a \rangle = G$. If $\langle a \rangle = G$ then we say that a is a **generator** for G.

Theorem. If G and H are isomorphic groups and G is cyclic then H is cyclic.

Theorem. Let a be an element of group G.

1. $o(a) = \infty \implies \langle a \rangle \cong \mathbb{Z}$.
2. $o(a) = n \in \mathbb{N} \implies \langle a \rangle \cong \mathbb{Z}_n$

Cayley's Theorem. If G is a finite group of order n, then there is a subgroup H of S_n such that $G \cong H$.

66. Let $\mathbb{Z}_{17}$ be the ring of integers modulo 17, and let $\mathbb{Z}_{17}{}^{\times}$ be the group of units of $\mathbb{Z}_{17}$ under multiplication. Which of the following are generators of $\mathbb{Z}_{17}{}^{\times}$?

I. 5

II. 8

III. 16

(A) None (B) I only (C) II only (D) III only (E) I, II, and III

Solution 66. (B) We need to pick elements of order 16 in $\mathbb{Z}/17^{\times}$. It is easy to rule out $16 \equiv -1$, since -1 has order 2. We see that $5^2 = 25 \equiv 8$, so there's no way that 8 can be a generator. We just need to verify that the order of 5 is more than 8, so we can check 5^8:

$$5^4 = 8^2 = 64 \equiv -4, \quad 5^8 = (-4)^2 = 16 \neq 1.$$

That makes 5 a generator.

Chapter 8: Cosets and Lagrange's Theorem

Let G be a group and let H be subgroup of G. For each element a of G we define

$$aH = \{ah \mid h \in H\}$$

We call aH the **coset of H in G generated by a.**

Let $a, b \in G$. Then

1. $a \in aH$ (since H must contain an identity; specifically, the identity of G)
2. $|aH| = |H|$ (since ah is unique)
3. $aH \cap bH \neq \emptyset \implies aH = bH$

Lagrange's Theorem. If G is a finite group and $H \leq G$ then $|H|$ divides $|G|$.

Any group of prime order is cyclic; therefore, there is only one such group up to isomorphism.

Exercise 3. Use Lagrange's theorem to prove that any group of prime order is cyclic.

Proof. Let G be a group whose order is a prime p. Since $p > 1$, there is an element $a \in G$ such that $a \neq e$. The group $\langle a \rangle$ generated by a is a subgroup of G. By Lagrange's theorem, the order of $\langle a \rangle$ divides $|G|$. But the only divisors of $|G| = p$ are 1 and p. Since $a \neq e$ we have $|\langle a \rangle| > 1$, so $|\langle a \rangle| = p$. Hence $\langle a \rangle = G$ and G is cyclic. □

We say that there are k **isomorphism classes of groups of order** n if there are k groups $G_1, G_2, \ldots, G_k$ such that

1. if $i \neq j$ then G_i and G_j are not isomorphic, and
2. Every group of order n is isomorphic to G_i for some $i \in \{1, 2, \ldots, k\}$.

This is sometimes expressed by saying that "there are k groups of order n up to isomorphism" or that "there are k non-isomorphic groups of order n."

12. For which integers n such that $3 \leq n \leq 11$ is there only one group of order n (up to isomorphism) ?

    (A) For no such integer n
    (B) For 3, 5, 7, and 11 only
    (C) For 3, 5, 7, 9, and 11 only
    (D) For 4, 6, 8, and 10 only
    (E) For all such integers n

Solution 12. (B) Any group of prime order is necessarily cyclic, and hence there is only one up to isomorphism. This limits are choices to (B), (C), and (E). But there are two groups of order 9 (at least): $\mathbb{Z}/3 \times \mathbb{Z}/3$ and $\mathbb{Z}/9$. This makes (B) our only option.

In more advanced courses in algebra, it is shown that the number of isomorphism classes of groups of order n for $n \leq 17$ is given by the following table:

Order :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Number :	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1

This table means, for example, that one may find 14 groups of order 16 such that every group of order 16 is isomorphic to one and only one of these 14 groups.

There is only one isomorphism class of groups of order n if n is prime. But there are some non-primes that have this property; for example, 15.

The Fundamental Theorem of Finite Abelian Groups. If G is a finite abelian group of order at least 2, then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_s^{n_s}}$$

where for each i, p_i is a prime and n_i is a positive integer. Moreover, the prime powers $p_i^{n_i}$ are unique except for the order of the factors.

If the group G in the above theorem has order n then

$$n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_2}$$

So the p_i may be obtained from the prime factorization of the order of the group G. These primes are not necessarily distinct, so we cannot say what the n_i are. However, we can find all possible choices for the n_i. For example, if G is an abelian group of order $72 = 3^2 \cdot 2^3$ then G is isomorphic to one and only one of the following groups. Note that each corresponds to a way of factoring 72 as a product of prime powers.

$\mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 9 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 9 \cdot 4 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_8$	$72 = 9 \cdot 8$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 4 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8$	$72 = 3 \cdot 3 \cdot 8$

Thus there are exactly 6 non-isomorphic abelian groups of order 72.

Corollary. For $n \geq 2$, the number of isomorphism classes of abelian groups of order n is equal to the number of ways to factor n as a product of prime powers (where the order of the factors does not count).

Chapter 9: Introduction to Ring Theory

Definition 9.1 *A **ring** is an ordered triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are binary operations on R satisfying the following properties:*

A1 $a + (b + c) = (a + b) + c$ *for all* a, b, c *in* R.

A2 $a + b = b + a$ *for all* a, b *in* R.

A3 *There is an element* $0 \in R$ *satisfying* $a + 0 = a$ *for all* a *in* R.

A4 *For every* $a \in R$ *there is an element* $b \in R$ *such that* $a + b = 0$.

M1 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* a, b, c *in* R.

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* a, b, c *in* R.

D2 $(b + c) \cdot a = b \cdot a + c \cdot a$ *for all* a, b, c *in* R.

Terminology If $(R, +, \cdot)$ is a ring, the binary operation $+$ is called *addition* and the binary operation $\cdot$ is called *multiplication. In the future we will usually write ab instead of* $a \cdot b$. The element 0 mentioned in A3 is called the **zero** of the ring. Note that we have not assumed that 0 behaves like a *zero*, that is, we have not assumed that $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$. What A3 says is that 0 is an identity with respect to addition. Note that *negative* (as the opposite of *positive*) has no meaning for most rings. We do not assume that multiplication is commutative and we have not assumed that there is an identity for multiplication, much less that elements have inverses with respect to multiplication.

23. Let $(\mathbb{Z}_{10}, +, \cdot)$ be the ring of integers modulo 10, and let S be the subset of $\mathbb{Z}_{10}$ represented by $\{0, 2, 4, 6, 8\}$. Which of the following statements is FALSE?

    (A) $(S, +, \cdot)$ is closed under addition modulo 10.

    (B) $(S, +, \cdot)$ is closed under multiplication modulo 10.

    (C) $(S, +, \cdot)$ has an identity under addition modulo 10.

    (D) $(S, +, \cdot)$ has no identity under multiplication modulo 10.

    (E) $(S, +, \cdot)$ is commutative under addition modulo 10.

Solution 23. (D) Examining the choices, we see $S \subset \mathbb{Z}/10$ is a subgroup of an abelian group. Therefore it still have an additive identity and the operation is commutative. It is also closed under addition and multiplication. While S does not contain the multiplicative identity of $\mathbb{Z}/10$, it does have a multiplicative identity. $6 \in S$ is such an identity, as

$$6x = (5+1)x = 5x + x.$$

Since $x \in S$ are all even, $5x = 0$, so $6x = x$.

50. Let R be a ring and let U and V be (two-sided) ideals of R. Which of the following must also be ideals of R?

I. $U + V = \{u + v : u \in U \text{ and } v \in V\}$

II. $U \cdot V = \{uv : u \in U \text{ and } v \in V\}$

III. $U \cap V$

(A) II only (B) III only (C) I and II only (D) I and III only (E) I, II, and III

Solution 50. (D) The sum of the ideals is still an ideal: it is clearly closed under addition (using commutativity of addition), and still under left and right multiplication due to the distributive property. The intersection of ideals is still an ideal, which is not too hard to work out. The product of ideals, however, need not be closed under addition. Consider, for example, $R = \mathbb{Z}[X]$, $U = (2, X)$, and $V = (3, X)$ (the ideals generated by two elements). Then we know that $-2X \in U \cdot V$ and $3X \in U \cdot V$, and hence we should expect $3X - 2X = X \in U \cdot V$. However, there is no way to get X as the product of an element of U and an element of V.

18. Let V be the real vector space of all real 2×3 matrices, and let W be the real vector space of all real 4×1 column vectors. If T is a linear transformation from V onto W, what is the dimension of the subspace $\{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}$?

(A) 2 (B) 3 (C) 4 (D) 5 (E) 6

Solution 18. (A) We see that $\dim V = 6$ and $\dim W = 4$. Since $\dim \operatorname{im} T = \dim W = 4$, we must have $\dim \ker T = 6 - 4 = 2$.

Miscellaneous

6. Which of the following circles has the greatest number of points of intersection with the parabola $x^2 = y + 4$?

(A) $x^2 + y^2 = 1$

(B) $x^2 + y^2 = 2$

(C) $x^2 + y^2 = 9$

(D) $x^2 + y^2 = 16$

(E) $x^2 + y^2 = 25$

Solution 6. (C) We can try to do this algebraically, but non-algebraically is simpler. Graphing $y = x^2 - 4$ shows that the graph crosses the x-axis at ± 2. Therefore a circle of radius 1 or $\sqrt{2}$ will not intersect the parabola at all. A circle of radius 3 will intersect four times – twice above and twice below the x-axis. A circle of radius 4 will only intersect at one point below the x-axis (and twice above), and a circle of radius 5 will only intersect at the two points above.

19. If z is a complex variable and $\overline{z}$ denotes the complex conjugate of z, what is $\lim_{z \to 0} \frac{(\overline{z})^2}{z^2}$?

(A) 0 (B) 1 (C) i (D) ∞ (E) The limit does not exist.

Solution 19. (E) Let us represent $z = a + bi$. Then our limit becomes

$$\lim_{(a,b) \to 0} \frac{(a - bi)^2}{(a + bi)^2} = \lim_{(a,b) \to 0} \frac{a^2 - b^2 - 2abi}{a^2 - b^2 + 2abi}.$$

If we let $a = 0$ (for instance), it is easy to see that the limit is equal to 1. However, if we let $a = b$, then our limit becomes

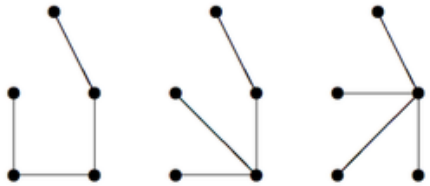
$$\lim_{a \to 0} \frac{-2a^2 i}{2a^2 i} = -1.$$

Therefore the limit does not exist.

29. A tree is a connected graph with no cycles. How many nonisomorphic trees with 5 vertices exist?

(A) 1 (B) 2 (C) 3 (D) 4 (E) 5

Solution 29. (C) It's probably easiest to draw this out for yourself. The maximum degree of any vertex is 2, 3, or 4. If there is a vertex of degree 4, then our tree looks like a star. If the maximum degree of any vertex is 2, then we have a straight line. In the middle case, we obtain a 3-pointed star to which we attach one more vertex – the choice of branch yields isomorphic graphs. See Figure 1.



38. The maximum number of acute angles in a convex 10-gon in the Euclidean plane is

(A) 1 (B) 2 (C) 3 (D) 4 (E) 5

Solution 38. (C) The total angle measure of a 10-gon is $180 \cdot 8 = 1440°$. If the polygon is to be convex, all angles must be less than $180°$. If we have 5 acute angles, then the remaining 5 angles would have to make up for $> 1440 - 5 \cdot 90 = 990$ degrees. This is impossible to do and remain convex. If we have 4 acute angles, the remaining 6 angles need to make up for $> 1440 - 4 \cdot 90 = 1080$ degrees. This is our edge case, so the answer must be 3 acute angles.

45. How many positive numbers x satisfy the equation $\cos(97x) = x$?

(A) 1 (B) 15 (C) 31 (D) 49 (E) 96

Solution 45. (C) Certainly our solutions are concentrated in $[0, 1]$. We know that every $2\pi/97$ units in x, we get another period of $\cos(97x)$, and each period must meet $y = x$ twice. Therefore there are

$$\frac{1}{2\pi/97} = \frac{97}{2\pi} \approx \frac{97}{6.3} \approx 15$$

periods in $[0, 1]$ and about 30 meetings. There's only one answer in that range, so we'll stick with it.