SURA'S

TRB

MATHEMATICS (PG)

- ❑ ALGEBRA
- ❑ REAL ANALYSIS
- ❑ FOURIER SERIES AND FOURIER INTEGRALS
- ❑ DIFFERENTIAL GEOMETRY
- ❑ OPERATIONS RESEARCH
- ❑ FUNCTIONAL ANALYSIS
- ❑ COMPLEX ANALYSIS
- ❑ DIFFERENTIAL EQUATIONS
- ❑ STATISTICS

SURA COLLEGE OF COMPETITION
Chennai

E 164

TRB MATHEMATICS (PG)

ISBN: 978-93-87150-55-3
Code : E 164

SURA COLLEGE OF COMPETITION

Head Office: 1620, 'J' Block, 16th Main Road, Anna Nagar,
Chennai - 600 040. Phones: 044-48629977, 42043273

Printed at Shankar Printers, Chennai - 600 042 and Published by
V.V.K.Subburaj for Sura College of Competition
1620, 'J' Block, 16th Main Road, Anna Nagar, Chennai - 600 040.
Phones: 044-48629977
email: enquiry@surabooks.com; suracollege@gmail.com;
website: www.surabooks.com

CONTENTS

■❖◆❖■

SYLLABUS FOR THE POST OF WRITTEN RECRUITMENT TEST
FOR THE POST OF POSTGRADUATE ASSISTANTS
IN TAMIL NADU HIGHER SECONDARY EDUCATIONAL SERVICE.

Syllabus: MATHS (Subject Code: P03)

Unit-I – MODERN LITERATURE (1400-1600)

Unit-I - Algebra

Groups – Examples – Cyclic Groups- Permulation Groups – Lagrange's theorem- Cosets – Normal groups - Homomorphism – Theorems – Cayley's theorem - Cauchy's Theorem - Sylow's theorem - Finitely Generated Abelian Groups – Rings- Euclidian Rings- Polynomial Rings- U.F.D. - Quotient - Fields of integral domains- Ideals- Maximal ideals - Vector Spaces - Linear independence and Bases - Dual spaces - Inner product spaces - Linear transformation – rank - Characteristic roots of matrices - Cayley Hamilton Theorem - Canonical form under equivalence – Fields - Characteristics of a field - Algebraic extensions - Roots of Polynomials - Splitting fields - Simple extensions – Elements of Galois theory- Finite fields.

Unit-II - Real Analysis

Cardinal numbers - Countable and uncountable cordinals - Cantor's diagonal process -Properties of real numbers - Order - Completeness of R-Lub property in R-Cauchy sequence - Maximum and minimum limits of sequences - Topology of R.Heine Borel - Bolzano Weierstrass - Compact if and only if closed and bounded - Connected subset of R-Lindelof's covering theorem - Continuous functions in relation to compact subsets and connected subsets- Uniformly continuous function – Derivatives - Left and right derivatives - Mean value theorem - Rolle's theorem- Taylor's theorem- L' Hospital's Rule - Riemann integral - Fundamental theorem of Calculus –Lebesgue measure and Lebesque integral on R'Lchesque integral of Bounded Measurable function - other sets of finite measure - Comparison of Riemann and Lebesque integrals - Monotone convergence theorem - Repeated integrals.

Unit-III - Fourier series and Fourier Integrals

Integration of Fourier series - Fejer's theorem on (C.1) summability at a point - Fejer's-Lebsque theorem on (C.1) summability almost everywhere – Riesz-Fisher theorem -

Bessel's inequality and Parseval's theorem - Properties of Fourier co-efficients - Fourier transform in L (-D, D) - Fourier Integral theorem - Convolution theorem for Fourier transforms and Poisson summation formula.

Unit-IV - Differential Geometry

Curves in spaces - Serret-Frenet formulas - Locus of centers of curvature - Spherical curvature - Intrinsic equation – Helices - Spherical indicatrix surfaces – Envelope - Edge of regression - Developable surfaces associated to a curve - first and second fundamental forms - lines of curvature - Meusnieu's theorem - Gaussian curvature - Euler's theorem - Duplin's Indicatrix - Surface of revolution conjugate systems - Asymptritic lines - Isolmetric lines – Geodesics.

Unit-V - Operations Research

Linear programming - Simplex Computational procedure - Geometric interpretation of the simplex procedure - The revised simplex method - Duality problems - Degeneracy procedure - Peturbation techniques - integer programming - Transportation problem – Non-linear programming - The convex programming problem - Dyamic programming - Approximation in function space, successive approximations - Game theory - The maximum and minimum principle - Fundamental theory of games - queuing theory / single server and multi server models (M/G/I), (G/M/I), (G/G1/I) models, Erlang service distributions cost Model and optimization - Mathematical theory of inventory control - Feed back control in inventory management - Optional inventory policies in deterministic models - Storage models - Damtype models - Dams with discrete input and continuous output - Replacement theory - Deterministic Stochostic cases - Models for unbounded horizons and uncertain case - Markovian decision models in replacement theory - Reliability - Failure rates - System reliability - Reliability of growth models - Network analysis - Directed net work - Max flowmin cut theorem - CPM-PERT - Probabilistic condition and decisional network analysis.

Unit-VI - Functional Analysis

Banach Spaces - Definition and example - continuous linear transformations - Banach theorem - Natural embedding of X in X - Open mapping and closed graph theorem - Properties of conjugate of an operator - Hilbert spaces - Orthonormal bases - Conjugate

space H - Adjoint of an operator - Projections l^2 as a Hilbert space – l^p space - Holders and Minkowski inequalities - Matrices – Basic operations of matrices - Determinant of a matrix - Determinant and spectrum of an operator - Spectral theorem for operators on a finite dimensional Hilbert space - Regular and singular elements in a Banach Algebra – Topological divisor of zero - Spectrum of an element in a Branch algebra - the formula for the spectral radius radical and semi simplicity.

Unit-VII - Complex Analysis

Introduction to the concept of analytic function - limits and continuity - analytic functions - Polynomials and rational functions elementary theory of power series – Maclaurin's series - uniform convergence power series and Abel's limit theorem - Analytic functions as mapping - conformality arcs and closed curves - Analytical functions in regions - Conformal mapping - Linear transformations - the linear group, the cross ratio and symmetry - Complex integration - Fundamental theorems - line integrals - rectifiable arcs - line integrals as functions of arcs - Cauchy's theorem for a rectangle, Cauchy's theorem in a Circular disc, Cauchy's integal formula - The index of a point with respect to a closed curve, the integral formula - higher derivatives - Local properties of Analytic functions and removable singularities- Taylor's theorem - Zeros and Poles - the local mapping and the maximum modulus Principle.

Unit-VIII - Differential Equations

Linear differential equation - constant co-efficients - Existence of solutions – Wrongskian - independence of solutions - Initial value problems for second order equations - Integration in series - Bessel's equation - Legendre and Hermite Polynomials - elementary properties - Total differential equations - first order partial differential equation - Charpits method.

Unit-IX - Statistics - I

Statistical Method - Concepts of Statistical population and random sample - Collections and presentation of data - Measures of location and dispersion - Moments and shepherd correction – cumulate - Measures of skewness and Kurtosis - Curve fitting by least squares – Regression - Correlation and correlation ratio - rank correlation - Partial correlation - Multiple correlation coefficient - Probability Discrete - sample

space, events - their union - intersection etc. - Probability classical relative frequency and axiomatic approaches - Probability in continuous probability space - conditional probability and independence - Basic laws of probability of combination of events - Baye's theorem - probability functions - Probability density functions - Distribution function - Mathematical Expectations - Marginal and conditional distribution - Conditional expectations.

Unit-X - Statistics-II

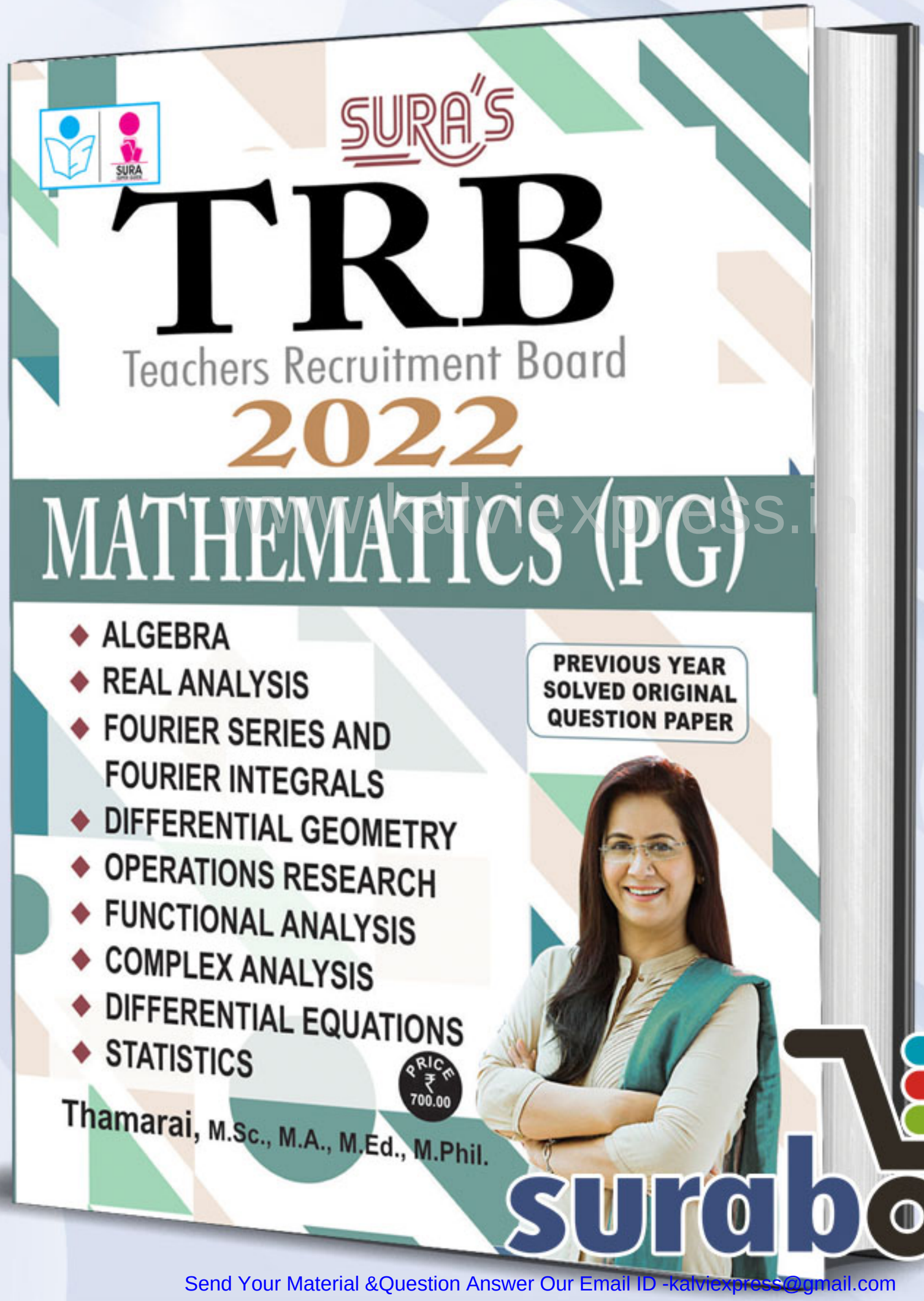
Probability distributions – Binomial, Poisson, Normal, Gama, Beta, Cauchy, Multinomial Hypergeometric, Negative Binomial - Chehychev's lemma (weak) law of large numbers - Central limit theorem for independent identical variates, Standard Errors - sampling distributions of t, F and Chi square - and their uses in tests of significance - Large sample tests for mean and proportions - Sample surveys - Sampling frame - sampling with equal probability with or without replacement - stratified sampling - Brief study of two stage systematic and cluster sampling methods - regression and ratio estimates - Design of experiments, principles of experimentation - Analysis of variance - Completely randomized block and latin square designs.

www.kalviexpress.in

SURA'S

TRB

Mathematics (PG)



surabooks.com

Unit - I

Algebra

TEST - 1

1. Let V be an inner product space and v_1, v_2, v_3 be vectors in V with $\langle v_1, v_2\rangle = 3$, $\langle v_2, v_3\rangle = -2$, $\langle v_1, v_3\rangle = 1$ and $\langle v_1, v_1\rangle = 1$. Calculate

   (a) $\langle v_1, 2v_2 + 3v_3\rangle$

   (b) $\langle 2v_1 - v_2, v_1 + v_3\rangle$.

   Suppose also that $\langle v_2, v_1 + v_2\rangle = 13$. Calculate

   (c) $\|v_2\|$.

2. Let V be an inner product space, $u, v \in V$, $\underline{0}$ the zero vector in V and $\alpha \in \mathbb{R}$. Prove that
   (a) $\langle \underline{0}, u\rangle = 0$; (b) $\|\alpha u\| = |\alpha|\,\|u\|$;
   (c) $\|u\| = \|-u\|$; (d) $\|u+v\|^2 + \|u-v\|^2 = 2(\|u\|^2 + \|v\|^2)$

3. By using the Cauchy-Schwarz inequality show that if $a_1, a_2, \ldots, a_n$ are positive real numbers, then
$$(a_1 + a_2 + \ldots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}\right) \geq n^2$$

4. Express $(1,2,3)$ as a linear combination of the vectors in the orthogonal basis
$$\{(1,-2,1), (2,1,0), (-1,2,5)\}.$$

5. Find an orthonormal basis for Span$\{(1,0,1,0), (1,1,2,0), (0,2,0,1)\}$ in $\mathbb{R}^4$.

6. Let the vector space P_2 have the inner product $\langle p(x), q(x)\rangle = \int_0^1 p(x)\,q(x)\,dx$. Apply the Gram-Schmidt procedure to transform the standard basis $1, x, x^2$ to an orthonormal basis.

7. Find an orthogonal basis for $\mathbb{R}^4$ containing the vectors $(2,1,-5,0)$ and $(3,-1,1,0)$.

8. Let S denote the family of vectors in $\mathbb{R}^3$ corresponding to points on the plane $2x - y + z = 0$

   (a) Find an orthonormal basis $\{u_1, u_2\}$ for S.

   (b) Find u_3 such that $\{u_1, u_2, u_3\}$ is an orthonormal basis for $\mathbb{R}^3$.

9. Let $\{u_1, \ldots, u_n\}$ be an orthonormal family of vectors in an inner product space V. Prove that $\|u_1 + \ldots + u_n\| = \sqrt{n}$.

10. Let V be an inner product space and $u, v_1, v_2, \ldots, v_n \in V$. Prove that if u is orthogonal to $v_1, v_2, \ldots, v_n$, then u is orthogonal to Span$\{v_1, v_2, \ldots, v_n\}$.

11. Prove that if $\langle u, v\rangle$ is the Euclidean inner product on $\mathbb{R}^n$ and if A is an n x n matrix then $\langle u, Av\rangle = \langle A^t u, v\rangle$. Hint: Notice that $\langle u, v\rangle = u^t v$ thinking of u and v as n x 1 matrices.

Solutions

1. (a) $\langle v_1, 2v_2+3v_3\rangle = 2\langle v_1,v_2\rangle + 3\langle v_1,v_3\rangle = 6+3=9$

   (b) $\begin{aligned}\langle 2v_1-v_2, v_1+v_3\rangle &= 2\langle v_1,v_1\rangle + 2\langle v_1,v_3\rangle - \langle v_2,v_1\rangle - \langle v_2,v_3\rangle \\ &= 2\langle v_1,v_1\rangle + 2\langle v_1,v_3\rangle - \langle v_1,v_2\rangle - \langle v_2,v_3\rangle \\ &= 2+2-3+2=3\end{aligned}$

   (c) $\begin{aligned}\langle v_2, v_1+v_2\rangle &= 13 \\ \text{so}\quad \langle v_2,v_1\rangle + \langle v_2,v_2\rangle &= 13 \\ \langle v_1,v_2\rangle + \langle v_2,v_2\rangle &= 13 \\ 3+\|v_2\|^2 &= 13 \\ \text{Hence}\quad \|v_2\| &= \sqrt{10}\end{aligned}$

2. (a) $\langle \underline{0}, u\rangle = \langle 0\underline{0}, u\rangle = 0\langle \underline{0}, u\rangle = 0$

   (b) $\|\alpha u\|^2 = \langle \alpha u, \alpha u\rangle = \alpha^2\langle u,u\rangle = \alpha^2\|u\|^2$
   So $\|\alpha u\| = \sqrt{\alpha^2}\|u\| = |\alpha|\|u\|$

   (c) $\|-u\| = \|(-1)u\| = |-1|\|u\| = \|u\|$

   (d) $\begin{aligned}\|u+v\|^2+\|u-v\|^2 &= \langle u+v,u+v\rangle + \langle u-v,u-v\rangle \\ &= \langle u,u\rangle + 2\langle u,v\rangle + \langle v,v\rangle + \langle u,u\rangle - 2\langle u,v\rangle + \langle v,v\rangle \\ &= 2(\langle u,u\rangle + \langle v,v\rangle) \\ &= 2(\|u\|^2+\|v\|^2)\end{aligned}$

3. Let $\underline{u} = (\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})$ and $\underline{v} = (1/\sqrt{a_1}, 1/\sqrt{a_2}, \ldots, 1/\sqrt{a_n})$. $\underline{u}$ and $\underline{v}$ are vectors in $\mathbb{R}^n$; applying the Cauchy–Schwarz inequality we have:

   $$|\langle \underline{u}, \underline{v}\rangle| \leq \|\underline{u}\|\|\underline{v}\|$$

   i.e. $\begin{aligned}\sqrt{a_1}\tfrac{1}{\sqrt{a_1}} + \sqrt{a_2}\tfrac{1}{\sqrt{a_2}} + \ldots + \sqrt{a_n}\tfrac{1}{\sqrt{a_n}} &\leq (a_1+a_2+\ldots+a_n)^{\frac{1}{2}}(\tfrac{1}{a_1}+\tfrac{1}{a_2}+\ldots+\tfrac{1}{a_n})^{\frac{1}{2}} \\ n &\leq (a_1+a_2+\ldots+a_n)^{\frac{1}{2}}(\tfrac{1}{a_1}+\tfrac{1}{a_2}+\ldots+\tfrac{1}{a_n})^{\frac{1}{2}} \\ n^2 &\leq (a_1+a_2+\ldots+a_n)(\tfrac{1}{a_1}+\tfrac{1}{a_2}+\ldots+\tfrac{1}{a_n})\end{aligned}$

4. Suppose $(1,2,3) = c_1(1,-2,1) + c_2(2,1,0) + c_3(-1,2,5)$

   Then $c_1 = \dfrac{\begin{pmatrix}1\\2\\3\end{pmatrix}\cdot\begin{pmatrix}1\\-2\\1\end{pmatrix}}{\begin{pmatrix}1\\-2\\1\end{pmatrix}\cdot\begin{pmatrix}1\\-2\\1\end{pmatrix}} = \frac{0}{6} = 0$

   $c_2 = \dfrac{\begin{pmatrix}1\\2\\3\end{pmatrix}\cdot\begin{pmatrix}2\\1\\0\end{pmatrix}}{\begin{pmatrix}2\\1\\0\end{pmatrix}\cdot\begin{pmatrix}2\\1\\0\end{pmatrix}} = \frac{4}{5}$

   $c_3 = \dfrac{\begin{pmatrix}1\\2\\3\end{pmatrix}\cdot\begin{pmatrix}-1\\2\\5\end{pmatrix}}{\begin{pmatrix}-1\\2\\5\end{pmatrix}\cdot\begin{pmatrix}-1\\2\\5\end{pmatrix}} = \frac{18}{30} = \frac{3}{5}$

   So $(1,2,3) = 0(1,-2,1) + \frac{4}{5}(2,1,0) + \frac{3}{5}(-1,2,5)$.

5. The set of vectors $\{(1,0,1,0),(1,1,2,0),(0,2,0,1)\}$ is linearly independent so forms a basis for $span\{(1,0,1,0),(1,1,2,0),(0,2,0,1)\}$. Apply the Gram–Schmidt procedure to this set:
   We have $\underline{u}_1 = (1,0,1,0)$, $\underline{u}_2 = (1,1,2,0)$, $\underline{u}_3 = (0,2,0,1)$.

Let $\underline{u}'_1 = \underline{u}_1,\ \underline{v}_1 = \frac{\underline{u}'_1}{\|\underline{u}'_1\|} = \frac{1}{\sqrt{2}}(1,0,1,0)$

Let $\underline{u}'_2 = \underline{u}_2 - \langle \underline{u}_2, \underline{v}_1\rangle \underline{v}_1 = (1,1,2,0) - \frac{3}{\sqrt{2}}\frac{1}{\sqrt{2}}(1,0,1,0) = (-\frac{1}{2},1,\frac{1}{2},0)$

$\underline{v}_2 = \frac{\underline{u}'_2}{\|\underline{u}'_2\|} = \frac{1}{\sqrt{6}}(-1,2,1,0)$

Let $\underline{u}'_3 = \underline{u}_3 - \langle \underline{u}_3, \underline{v}_1\rangle \underline{v}_1 - \langle \underline{u}_3, \underline{v}_2\rangle \underline{v}_2 = (0,2,0,1) - 0\underline{v}_1 - \frac{4}{\sqrt{6}}\frac{1}{\sqrt{6}}(-1,2,1,0) = (\frac{2}{3},\frac{2}{3},-\frac{2}{3},1)$

$\underline{v}_3 = \frac{\underline{u}'_3}{\|\underline{u}'_3\|} = \sqrt{\frac{9}{21}}(\frac{2}{3},\frac{2}{3},-\frac{2}{3},1) = \frac{1}{\sqrt{21}}(2,2,-2,3)$

Thus an orthonormal basis for $span\{(1,0,1,0),(1,1,2,0),(0,2,0,1)\}$ is

$$\{\frac{1}{\sqrt{2}}(1,0,1,0), \frac{1}{\sqrt{6}}(-1,2,1,0), \frac{1}{\sqrt{21}}(2,2,-2,3)\}.$$

6. Apply the Gram–Schmidt procedure with $u_1 = 1$, $u_2 = x$, $u_3 = x^2$.

Let $u'_1 = u_1 = 1$

$$v_1 = \frac{u'_1}{\|u'_1\|} = \frac{1}{\left\{\int_0^1 1^2 dx\right\}^{\frac{1}{2}}} = 1$$

Let $u'_2 = u_2 - \langle u_2, v_1\rangle v_1 = x - (\int_0^1 x dx).1 = x - \frac{1}{2}$

$$v_2 = \frac{u'_2}{\|u'_2\|} = \frac{x-\frac{1}{2}}{\left\{\int_0^1 (x-\frac{1}{2})^2 dx\right\}^{\frac{1}{2}}} = \frac{x-\frac{1}{2}}{\left\{\left[\frac{1}{3}(x-\frac{1}{2})^3\right]_0^1\right\}^{\frac{1}{2}}} = \frac{x-\frac{1}{2}}{(\frac{1}{12})^{\frac{1}{2}}} = \sqrt{12}(x-\frac{1}{2})$$

Let $u'_3 = u_3 - \langle u_3, v_1\rangle v_1 - \langle u_3, v_2\rangle v_2$

$$= x^2 - (\int_0^1 x^2 dx).1 - 12(\int_0^1 x^2(x-\frac{1}{2})dx)(x-\frac{1}{2})$$

$$= x^2 - \frac{1}{3} - 12\left[\frac{x^4}{4} - \frac{x^3}{6}\right]_0^1 (x-\frac{1}{2})$$

$$= x^2 - \frac{1}{3} - 12 \times \frac{1}{12}(x-\frac{1}{2})$$

$$= x^2 - x + \frac{1}{6}$$

$$v_3 = \frac{u'_3}{\|u'_3\|}$$

Now $\|u'_3\| = \left\{\int_0^1 (x^2 - x + \frac{1}{6})^2 dx\right\}^{\frac{1}{2}}$

$$= \left\{\int_0^1 (x^4 - 2x^3 + \tfrac{4}{3}x^2 - \tfrac{1}{3}x + \tfrac{1}{36})dx\right\}^{\frac{1}{2}}$$

$$= \left\{\left[\tfrac{x^5}{5} - \tfrac{2x^4}{4} + \tfrac{4x^3}{9} - \tfrac{x^2}{6} + \tfrac{x}{36}\right]_0^1\right\}^{\frac{1}{2}}$$

$$= \left\{\tfrac{36-90+80-30+5}{180}\right\}^{\frac{1}{2}}$$

$$= \tfrac{1}{\sqrt{180}}$$

Hence $v_3 = \sqrt{180}(x^2 - x + \frac{1}{6})$. Thus an orthonormal basis for P_2 with this inner product is $\{1, \sqrt{12}(x-\frac{1}{2}), \sqrt{180}(x^2-x+\frac{1}{6})\}$.

7. $\{(2,1,-5,0),(3,-1,1,0)\}$ is an orthogonal set so normalising we obtain the orthonormal set $\{\frac{1}{\sqrt{30}}(2,1,-5,0), \frac{1}{\sqrt{11}}(3,-1,1,0)\}$. Now choose two linearly independent vectors not in the span of this set eg. $(0,0,0,1)$ and $(1,0,0,0)$.
$\{\frac{1}{\sqrt{30}}(2,1,-5,0), \frac{1}{\sqrt{11}}(3,-1,1,0), (0,0,0,1), (1,0,0,0)\}$ is a basis for $\mathbb{R}^4$; apply Gram–Schmidt to this basis:
Let $v_1 = \frac{1}{\sqrt{30}}(2,1,-5,0)$, $v_2 = \frac{1}{\sqrt{11}}(3,-1,1,0)$, $u_3 = (0,0,0,1)$ and $u_4 = (1,0,0,0)$.

Let $u_3' = u_3 - \langle u_3, v_1\rangle v_1 - \langle u_3, v_2\rangle v_2 = u_3 - 0v_1 - 0v_2 = u_3$

$$v_3 = \frac{u_3'}{\|u_3'\|} = (0,0,0,1)$$

$$\begin{aligned} \text{Let } u_4' &= u_4 - \langle u_4, v_1\rangle v_1 - \langle u_4, v_2\rangle v_2 - \langle u_4, v_3\rangle v_3 \\ &= (1,0,0,0) - \tfrac{2}{30}(2,1,-5,0) - \tfrac{3}{11}(3,-1,1,0) - 0 \\ &= \tfrac{1}{330}(16,68,20,0) = \tfrac{2}{165}(4,17,5,0) \end{aligned}$$

Hence an orthogonal basis for $\mathbb{R}^4$ containing $\{(2,1,-5,0),(3,-1,1,0)\}$ is $\{(2,1,-5,0),(3,-1,1,0),(0,0,0,1),(4,17,5,0)\}$.

8. (a) The vector $(1,0,-2)$ lies on the plane so let $u_1 = (1,0,-2)$.
Suppose $u_2 = (a,b,c)$. We require u_2 to lie on the plane so

$$2a - b + c = 0 \quad (1)$$

and that u_2 is orthogonal to u_1 i.e. $u_1.u_2 = 0$ hence

$$a - 2c = 0 \quad (2)$$

A solution to (1) and (2) is $c = 1, a = 2, b = 5$ so we can take $\underline{v}_2 = (2,5,1)$. So $\{(1,0,-2),(2,5,1)\}$ are orthogonal vectors in S. They are linearly independent (since they are orthogonal) and since S is a plane it has dimension 2 so these vectors form a basis for S. Hence $\{\frac{1}{\sqrt{5}}(1,0,-2), \frac{1}{\sqrt{30}}(2,5,1)\}$ is an orthonormal basis for S.

(b) The plane $2x - y + z = 0$ has normal $(2,-1,1)$ and so $u_3 = (2,-1,1)$ is orthogonal to the vectors in (a) above. Hence $\{\frac{1}{\sqrt{5}}(1,0,-2), \frac{1}{\sqrt{30}}(2,5,1), \frac{1}{\sqrt{6}}(2,-1,1)\}$ is an orthonormal basis for $\mathbb{R}^3$.

9.
$$\begin{aligned} \|u_1 + u_2 + \ldots + u_n\|^2 &= (u_1 + u_2 + \ldots + u_n, u_1 + u_2 + \ldots + u_n) \\ &= \langle u_1, u_1\rangle + \langle u_1, u_2\rangle + \ldots + \langle u_1, u_n\rangle \\ &\quad + \langle u_2, u_1\rangle + \langle u_2, u_2\rangle + \ldots + \langle u_2, u_n\rangle \\ &\quad + \ldots \\ &\quad + \langle u_n, u_1\rangle + \langle u_n, u_2\rangle + \ldots + \langle u_n, u_n\rangle \\ &= \langle u_1, u_1\rangle + \langle u_2, u_2\rangle + \ldots + \langle u_n, u_n\rangle \quad \text{since } \langle u_i, u_j\rangle = 0 \ \ i \neq j \\ &= n \quad \text{as } \langle u_i, u_i\rangle = 1 \quad i = 1, \ldots, n \end{aligned}$$

hence $\|u_1 + u_2 + \ldots + u_n\| = \sqrt{n}$.

10. Let $v \in span\{u_1, u_2, \ldots, u_n\}$.
Then $\exists\, c_1, c_2, \ldots, c_n \in \mathbb{R}$ such that $v = c_1u_1 + c_2u_2 + \ldots + c_nu_n$.
Now, $\langle u, v\rangle = \langle u, c_1u_1 + c_2u_2 + \ldots + c_nu_n\rangle$
$= c_1\langle u, u_1\rangle + c_2\langle u, u_2\rangle + \ldots + c_n\langle u, u_n\rangle$
$= 0$ since u is orthogonal to $u_1, u_2, \ldots, u_n$
Hence u is orthogonal to v for all $v \in span\{u_1, \ldots, u_n\}$.

11. $\langle u, Av\rangle = u^tAv$
$\langle A^tu, v\rangle = (A^tu)^tv = u^t(A^t)^tv = u^tAv$
So $\langle u, Av\rangle = \langle A^tu, v\rangle$.

TEST - 2

1. Find all solutions of the system of equations

$$\begin{aligned} -3x_1 + x_2 + 4x_3 &= -5 \\ x_1 + x_2 + x_3 &= 2 \\ -2x_1 + x_3 &= -3 \\ x_1 + x_2 - 2x_3 &= 5. \end{aligned}$$

2. Find the general solution of the system of equations

$$\begin{aligned} x + y - z + u + v &= 0 \\ 2x + y + 2z - u - 2v &= 0 \\ 4x + 3y + u &= 0 \\ 5x + 3y + 3z - u - 3v &= 0 \\ x - y + 7z - 5u - 7v &= 0. \end{aligned}$$

3. Find all solutions of the system of equations

$$\begin{aligned} x + 2y - z &= 2 \\ 2x + y + z &= 3 \\ x - y + 2z &= 2. \end{aligned}$$

4. Consider the system

$$\begin{aligned} 2x_1 - x_2 + 3x_3 &= a \\ 3x_1 + x_2 - 5x_3 &= b \\ -5x_1 - 5x_2 + 21x_3 &= c. \end{aligned}$$

Find conditions on a, b, c so that the system is inconsistent.

5. Determine all values of a for which the following system has
(i) no solution; (ii) a unique solution; (iii) infinitely many solutions:

$$\begin{aligned} x_1 + x_2 - x_3 &= 2 \\ x_1 + 2x_2 + x_3 &= 3 \\ x_1 + x_2 + (a^2 - 5)x_3 &= a. \end{aligned}$$

6. Find a homogeneous linear system of two equations such that

$$x_1 = 1, x_2 = -1, x_3 = 1, x_4 = 2$$

and

$$x_1 = 2, x_2 = 0, x_3 = 3, x_4 = -1$$

are solutions of the system.

7. By using Gaussian elimination find positive integers which satisfy

$$x + y + z = 9$$
$$x + 5y + 10z = 44.$$

8. Find an inconsistent linear system that has more unknowns than equations.

9. Carrying out as few computations as possible determine which of the following homogeneous systems have nontrivial solutions.

$$x_1 + x_2 + x_3 + x_4 = 0$$
$$x_1 - 4x_2 - 6x_3 + 5x_4 = 0$$
$$3x_1 + 5x_2 - 7x_3 + x_4 = 0$$

$$x_1 + x_2 + x_3 = 0$$
$$2x_2 + 3x_3 = 0$$
$$5x_3 = 0$$

$$x_1 + x_2 = 0$$
$$2x_1 + 2x_2 = 0$$

10. Consider the homogeneous system of equations, $A\underline{x} = \underline{0}$. Show that, if $\underline{x}_1$ and $\underline{x}_2$ are solutions of this system and λ is a real number, then $\underline{x}_1 + \underline{x}_2$ and $\lambda\underline{x}_1$ are also solutions of the system. Does the result hold for inhomogeneous systems ?

Solutions

1. The system has the same solutions as the systems corresponding to the arrays:

$$\left(\begin{array}{rrr|r} -3 & 1 & 4 & -5 \\ 1 & 1 & 1 & 2 \\ -2 & 0 & 1 & -3 \\ 1 & 1 & -2 & 5 \end{array}\right) r_1 \leftrightarrow r_2 \quad \left(\begin{array}{rrr|r} 1 & 1 & 1 & 2 \\ -3 & 1 & 4 & -5 \\ -2 & 0 & 1 & -3 \\ 1 & 1 & -2 & 5 \end{array}\right) \begin{array}{l} r_2 \to r_2 + 3r_1 \\ r_3 \to r_3 + 2r_1 \\ r_4 \to r_4 - r_1 \end{array}$$

$$\left(\begin{array}{rrr|r} 1 & 1 & 1 & 2 \\ 0 & 4 & 7 & 1 \\ 0 & 2 & 3 & 1 \\ 0 & 0 & -3 & 3 \end{array}\right) r_3 \to 2r_3 - r_2 \quad \left(\begin{array}{rrr|r} 1 & 1 & 1 & 2 \\ 0 & 4 & 7 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -3 & 3 \end{array}\right) r_4 \to r_4 - 3r_3 \quad \left(\begin{array}{rrr|r} 1 & 1 & 1 & 2 \\ 0 & 4 & 7 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

i.e. $\begin{array}{r} x_1 + x_2 + x_3 = 2 \\ 4x_2 + 7x_3 = 1 \\ -x_3 = 1 \end{array}$ So $x_3 = -1$, $x_2 = (1 - 7x_3)/4 = 2$, $x_1 = 2 - x_2 - x_3 = 1$. The system is consistent and has the unique solution $x_1 = 1, x_2 = 2, x_3 = -1$.

2. The system has the same solutions as the systems corresponding to

$$\left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 & -2 & 0 \\ 4 & 3 & 0 & 1 & 0 & 0 \\ 5 & 3 & 3 & -1 & -3 & 0 \\ 1 & -1 & 7 & -5 & -7 & 0 \end{array}\right) \begin{array}{l} r_2 \to r_2 - 2r_1 \\ r_3 \to r_3 - 4r_1 \\ r_4 \to r_4 - 5r_1 \\ r_5 \to r_5 - r_1 \end{array} \quad \left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 1 & 1 & 0 \\ 0 & -1 & 4 & -3 & -4 & 0 \\ 0 & -1 & 4 & -3 & -4 & 0 \\ 0 & -2 & 8 & -6 & -8 & 0 \\ 0 & -2 & 8 & -6 & -8 & 0 \end{array}\right) \begin{array}{l} r_3 \to r_3 - r_2 \\ r_4 \to r_4 - 2r_2 \\ r_5 \to r_5 - 2r_2 \end{array}$$

$$\left(\begin{array}{rrrrr|r} 1 & 1 & -1 & 1 & 1 & 0 \\ 0 & -1 & 4 & -3 & -4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \text{ i.e. } \begin{array}{r} x + y - z + u + v = 0 \\ -y + 4z - 3u - 4v = 0 \end{array}$$

Thus we obtain the solution $v = \alpha$, $u = \beta$, $z = \gamma$, $y = 4\gamma - 3\beta - 4\alpha$, $x = -y + z - u - v = -3\gamma + 2\beta + 3\alpha$ for any constants α, β, γ.

3. The system has the same solutions as the systems corresponding to

$$\left(\begin{array}{rrr|r} 1 & 2 & -1 & 2 \\ 2 & 1 & 1 & 3 \\ 1 & -1 & 2 & 2 \end{array}\right) \begin{array}{l} r_2 \to r_2 - 2r_1 \\ r_3 \to r_3 - r_1 \end{array} \quad \left(\begin{array}{rrr|r} 1 & 2 & -1 & 2 \\ 0 & -3 & 3 & -1 \\ 0 & -3 & 3 & 0 \end{array}\right) r_3 \to r_3 - r_2$$

$$\left(\begin{array}{rrr|r} 1 & 2 & -1 & 2 \\ 0 & -3 & 3 & -1 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

The last row corresponds to the equation $0x + 0y + 0z = 1$ which has no solution. Hence the system is inconsistent.

4. The system has the same solutions as the systems corresponding to the arrays:

$$\left(\begin{array}{rrr|r} 2 & -1 & 3 & a \\ 3 & 1 & -5 & b \\ -5 & -5 & 21 & c \end{array}\right) \begin{array}{l} r_2 \to 2r_2 - 3r_1 \\ r_3 \to 2r_3 + 5r_1 \end{array} \quad \left(\begin{array}{rrr|r} 2 & -1 & 3 & a \\ 0 & 5 & -19 & 2b - 3a \\ 0 & -15 & 57 & 2c + 5a \end{array}\right) r_3 \to r_3 + 3r_2$$

$$\left(\begin{array}{ccc|c} 2 & -1 & 3 & a \\ 0 & 5 & -19 & 2b-3a \\ 0 & 0 & 0 & -4a+6b+2c \end{array}\right)$$

Row 3 corresponds to the equation $0x_1+0x_2+0x_3=-4a+6b+2c$ so the system is inconsistent if and only if $-4a+6b+2c\neq 0$ i.e. $2a-3b-c\neq 0$.

5. The system has the same solutions as the systems corresponding to the following arrays:

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 2 \\ 1 & 2 & 1 & 3 \\ 1 & 1 & a^2-5 & a \end{array}\right) \begin{array}{l} r_2\to r_2-r_1 \\ r_3\to r_3-r_1 \end{array} \left(\begin{array}{ccc|c} 1 & 1 & -1 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & a^2-4 & a-2 \end{array}\right)$$

The last row corresponds to the equation $(a^2-4)x_3=a-2$. If $a^2-4\neq 0$, i.e. $a\neq\pm 2$ the system has a unique solution. If $a=2$ the last row becomes zero and the system has infinitely many solutions. If $a=-2$ the last row corresponds to $0x_1+0x_2+0x_3=-4$ so the system is inconsistent.

6. Consider the equation $ax_1+bx_2+cx_3+dx_4=0$. If $x_1=1,x_2=-1,x_3=1,x_4=2$ is a solution we must have $a-b+c+2d=0$ (1).
If $x_1=2,x_2=0,x_3=3,x_4=-1$ is a solution we must have $2a+3c-d=0$ (2).
(1) and (2) have the same solutions as the systems represented by

$$\left(\begin{array}{cccc|c} 1 & -1 & 1 & 2 & 0 \\ 2 & 0 & 3 & -1 & 0 \end{array}\right) r_2\to r_2-2r_1 \left(\begin{array}{cccc|c} 1 & -1 & 1 & 2 & 0 \\ 0 & 2 & 1 & -5 & 0 \end{array}\right)$$

i.e. $\begin{array}{l} a-b+c+2d=0 \\ 2b+c-5d=0 \end{array}$ Solutions are given by $d=\alpha$, $c=\beta$, $b=\frac{1}{2}(5\alpha-\beta)$, $a=\frac{1}{2}(\alpha-3\beta)$.
Each choice of α,β yields an equation with the desired property. Choosing $\alpha=0,\beta=1$ we obtain $a=-\frac{3}{2}$, $b=-\frac{1}{2},c=1,d=0$. Choosing $\alpha=1,\beta=0$ we obtain $a=\frac{1}{2},b=\frac{5}{2},c=0,d=1$. So an appropriate system of equations is

$$\begin{array}{l} -\frac{3}{2}x_1-\frac{1}{2}x_2+x_3=0 \\ \frac{1}{2}x_1+\frac{5}{2}x_2+x_4=0. \end{array}$$

7. The system has the same solutions as systems corresponding to the arrays

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 9 \\ 1 & 5 & 10 & 44 \end{array}\right) r_2\to r_2-r_1 \left(\begin{array}{ccc|c} 1 & 1 & 1 & 9 \\ 0 & 4 & 9 & 35 \end{array}\right)$$

i.e. $\begin{array}{ll} x+y+z=9 & (1) \\ 4y+9z=35 & (2) \end{array}$
Since x,y,z are positive integers (2) can not be satisfied unless $z<4$. Trying $z=1,2,3$ it is found that $z=3$, $y=2$, $x=4$ is the only positive integer solution.

8. Examples of inconsistent linear systems with more unknowns than equations:
a) $0x+0y=1$
b) $\begin{array}{l} x_1+x_2+x_3=1 \\ 2x_1+2x_2+2x_3=3 \end{array}$
There are many such systems, but none of them can be homogeneous.

9. A non-trivial solution is any solution other than the trivial solution $\underline{x}=\underline{0}$.

(a) The system is homogeneous with more unknowns than equations, so has (infinitely many) non-trivial solutions.

(b) $x_3 = 0 \Rightarrow x_2 = 0 \Rightarrow x_1 = 0$ so this system has no non-trivial solutions.

(c) The system has general solutions $x_2 = \alpha$, $x_1 = -\alpha$ where α is an arbitrary constant so the system has (infinitely many) non-trivial solutions.

10. $\begin{aligned} A(\underline{x}_1 + \underline{x}_2) &= A\underline{x}_1 + A\underline{x}_2 \quad \text{(by properties of matrices)} \\ &= \underline{0} + \underline{0} \quad \text{(since } \underline{x}_1 \text{ and } \underline{x}_2 \text{ are solutions of } A\underline{x} = \underline{0}) \\ &= \underline{0} \end{aligned}$

Hence $\underline{x}_1 + \underline{x}_2$ is a solution of $A\underline{x} = \underline{0}$.

Also $\begin{aligned} A(\lambda \underline{x}_1) &= \lambda A\underline{x}_1 \quad \text{(properties of matrices)} \\ &= \lambda \underline{0} \\ &= \underline{0} \end{aligned}$

So $\lambda \underline{x}_1$ is a solution of $A\underline{x} = \underline{0}$.

This is false for inhomogeneous systems. For example consider the system $x + y = 1$. i.e. $(1\ 1)\begin{pmatrix} x \\ y \end{pmatrix} = 1$

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are solutions, but $\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is not.

TEST - 3

1. Which of the following are linear transformations ?

   (a) $T_1 : \mathbb{R}^2 \to \mathbb{R}^2$ such that $T_1 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x \end{pmatrix}$

   (b) $T_2 : \mathbb{R}^2 \to \mathbb{R}^2$ such that $T_2 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x-y \end{pmatrix}$

   (c) $T_3 : \mathbb{R}^2 \to \mathbb{R}^2$ such that $T_3 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ \sin y \end{pmatrix}$

   (d) $T_4 : M_{22} \to M_{22}$ such that $T_4(A) = A^t$

   (e) $T_5 : M_{22} \to \mathbb{R}$ such that $T_5(A) = \det A$.

2. Let U and V be vector spaces and let $T : U \to V$ be a linear transformation. Which of the following statements are true and which are false ? Prove the statements that are true and provide counterexamples to those that are false.

   (a) If $\{u_1, \ldots, u_n\}$ is linearly dependent in U then $\{T(u_1), \ldots, T(u_n)\}$ is linearly dependent in V.

   (b) If $\{u_1, \ldots, u_n\}$ is linearly independent in U then $\{T(u_1), \ldots, T(u_n)\}$ is linearly independent in V.

   (c) If $\{u_1, \ldots, u_n\}$ span U then $\{T(u_1), \ldots, T(u_n)\}$ spans V.

3. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ such that $T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ 2x+y \end{pmatrix}$. Find the matrix which represents T

   (a) relative to the basis $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$; (b) relative to the basis $\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$.

4. Let $D : P_n \to P_n$ be the differentiation operator defined by

   $$D(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$$

   Find the matrix which represents D relative to the basis $\{1, x, \ldots, x^n\}$.

5. Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ such that $T \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x-y-z \\ x+3y+z \\ 3x-y-2z \end{pmatrix}$.

   Find bases for the range space and kernel of T.

6. Let $T : P_2 \to P_3$ be the linear transformation defined by $T(p(x)) = xp(x)$. Find the range space and kernel of T and hence determine the rank and nullity of T.

7. Give examples of linear transformations T as specified below.

   (a) $T : \mathbb{R}^5 \to \mathbb{R}^3$ has rank 2; (b) $T : M_{22} \to M_{22}$ has rank 3.

   In each case find the nullity of T and give bases for the null spaces and range spaces of T.

Solutions

1. (a) T_1 is a linear transformation:

Suppose $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \in \mathbb{R}^2, \alpha \in \mathbb{R}$.

$$\text{Then } T_1\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = T_1\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix}$$
$$= \begin{pmatrix} x_1+x_2 \\ x_1+x_2 \end{pmatrix}$$
$$= \begin{pmatrix} x_1 \\ x_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ x_2 \end{pmatrix}$$
$$= T_1\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + T_1\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

$$\text{and } T_1\left(\alpha\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right) = T_1\begin{pmatrix} \alpha x_1 \\ \alpha y_1 \end{pmatrix}$$
$$= \begin{pmatrix} \alpha x_1 \\ \alpha x_1 \end{pmatrix}$$
$$= \alpha\begin{pmatrix} x_1 \\ x_1 \end{pmatrix}$$
$$= \alpha T_1\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Hence T_1 is a linear transformation.

(b) T_2 is a linear transformation:

Suppose $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \in \mathbb{R}^2, \alpha \in \mathbb{R}$.

$$\text{Then } T_2\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = T_2\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix}$$
$$= \begin{pmatrix} x_1+x_2+y_1+y_2 \\ x_1+x_2-y_1-y_2 \end{pmatrix}$$
$$= \begin{pmatrix} x_1+y_1 \\ x_1-y_1 \end{pmatrix} + \begin{pmatrix} x_2+y_2 \\ x_2-y_2 \end{pmatrix}$$
$$= T_2\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + T_2\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

$$\text{and } T_2\left(\alpha\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right) = T_2\begin{pmatrix} \alpha x_1 \\ \alpha y_1 \end{pmatrix}$$
$$= \begin{pmatrix} \alpha x_1+\alpha y_1 \\ \alpha x_1-\alpha y_1 \end{pmatrix}$$
$$= \alpha\begin{pmatrix} x_1+y_1 \\ x_1-y_1 \end{pmatrix}$$
$$= \alpha T_1\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Hence T_2 is a linear transformation.

(c) T_3 is not a linear transformation (roughly speaking the problem is that $y \mapsto \sin y$ is not linear):

$$T_3\left(2\begin{pmatrix} 0 \\ \frac{\pi}{2} \end{pmatrix}\right) = T_3\begin{pmatrix} 0 \\ \pi \end{pmatrix} = \begin{pmatrix} \pi \\ \sin\pi \end{pmatrix} = \begin{pmatrix} \pi \\ 0 \end{pmatrix}$$

but, $2T_3\begin{pmatrix}0\\ \frac{\pi}{2}\end{pmatrix} = 2\begin{pmatrix}\frac{\pi}{2}\\ \sin\frac{\pi}{2}\end{pmatrix} = 2\begin{pmatrix}\frac{\pi}{2}\\ 1\end{pmatrix} = \begin{pmatrix}\pi\\ 2\end{pmatrix}$

So $T_3\left(2\begin{pmatrix}0\\ \frac{\pi}{2}\end{pmatrix}\right) \neq 2T_3\begin{pmatrix}0\\ \frac{\pi}{2}\end{pmatrix}$

So T_3 is not a linear transformation.

(d) T_4 is a linear transformation:

Suppose $A, B \in M_{22}$ and $\alpha \in \mathbb{R}$

Then $T_4(A+B) = (A+B)^t = A^t + B^t = T_4(A) + T_4(B)$

and $T_4(\alpha A) = (\alpha A)^t = \alpha A^t = \alpha T_4(A)$

(e) T_5 is not a linear transformation:

$T_5\left(\begin{pmatrix}1&0\\0&0\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix}\right) = T_5\begin{pmatrix}1&0\\0&1\end{pmatrix} = det\begin{pmatrix}1&0\\0&1\end{pmatrix} = 1$

But $T_5\begin{pmatrix}1&0\\0&0\end{pmatrix} + T_5\begin{pmatrix}0&0\\0&1\end{pmatrix} = det\begin{pmatrix}1&0\\0&0\end{pmatrix} + det\begin{pmatrix}0&0\\0&1\end{pmatrix} = 0+0=0$

So $T_5\left(\begin{pmatrix}1&0\\0&0\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix}\right) \neq T_5\begin{pmatrix}1&0\\0&0\end{pmatrix} + T_5\begin{pmatrix}0&0\\0&1\end{pmatrix}$

hence T_5 is not linear.

2. (a) True.

Suppose $\{u_1, u_2, \ldots, u_n\}$ is linearly dependent.

Then $\exists\, c_1, \ldots, c_n \in \mathbb{R}$ not all zero such that $c_1u_1 + c_2u_2 + \ldots + c_nu_n = \underline{0}$

Now $c_1T(u_1) + c_2T(u_2) + \ldots + c_nT(u_n) = T(c_1u_1 + c_2u_2 + \ldots + c_nu_n)$

$= T(\underline{0})$

$= \underline{0}$

So $\{T(u_1), T(u_2), \ldots, T(u_n)\}$ is linearly dependent.

(b) False.

Let $U = \mathbb{R}^2, V = \mathbb{R}^2, u_1 = \begin{pmatrix}1\\0\end{pmatrix}, u_2 = \begin{pmatrix}0\\1\end{pmatrix}$ and $T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\\x\end{pmatrix}$

Now, $\{u_1, u_2\}$ is a linearly independent set.

However $T\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$ and $T\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$

so $\{T(u_1), T(u_2)\} = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}\right\}$ which is a linearly dependent set.

(c) False.

Let $U = \mathbb{R}^2, V = \mathbb{R}^2, u_1 = \begin{pmatrix}1\\0\end{pmatrix}, u_2 = \begin{pmatrix}0\\1\end{pmatrix}$ and $T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\\x\end{pmatrix}$

Now $\{u_1, u_2\}$ spans $\mathbb{R}^2$.

However $T\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$ and $T\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$

so $\{T(u_1), T(u_2)\} = \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}\right\}$ which does not span $\mathbb{R}^2$.

3. (a) $T\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\2\end{pmatrix} = 1\begin{pmatrix}1\\0\end{pmatrix} + 2\begin{pmatrix}0\\1\end{pmatrix}$; $T\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}-1\\1\end{pmatrix} = -1\begin{pmatrix}1\\0\end{pmatrix} + 1\begin{pmatrix}0\\1\end{pmatrix}$

So the matrix is $\begin{pmatrix}1&-1\\2&1\end{pmatrix}$.

(b) $T\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}-1\\4\end{pmatrix}=c_1\begin{pmatrix}1\\2\end{pmatrix}+c_2\begin{pmatrix}1\\1\end{pmatrix}$ where $\begin{aligned}-1&=c_1+c_2 \quad (1)\\4&=2c_1+c_2 \quad (2)\end{aligned}$

$(2)-(1)$ gives $5=c_1$ so $c_2=-6$.

Hence $T\begin{pmatrix}1\\2\end{pmatrix}=5\begin{pmatrix}1\\2\end{pmatrix}-6\begin{pmatrix}1\\1\end{pmatrix}$

$T\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}0\\3\end{pmatrix}=c_1\begin{pmatrix}1\\2\end{pmatrix}+c_2\begin{pmatrix}1\\1\end{pmatrix}$ where $\begin{aligned}0&=c_1+c_2 \quad (1)\\3&=2c_1+c_2 \quad (2)\end{aligned}$

$(2)-(1)$ gives $c_1=3$ so $c_2=-3$.

Hence $T\begin{pmatrix}1\\1\end{pmatrix}=3\begin{pmatrix}1\\2\end{pmatrix}-3\begin{pmatrix}1\\1\end{pmatrix}$

So the matrix is $\begin{pmatrix}5&3\\-6&-3\end{pmatrix}$.

4. $\begin{aligned}D(1)&=0&&=0.1+0.x+\ldots+0.x^n\\D(x)&=1&&=1.1+0.x+\ldots+0.x^n\\D(x^2)&=2x&&=0.1+2.x+0.x^2+\ldots+0.x^n\\&\vdots\\D(x^n)&=nx^{n-1}&&=0.1+\ldots+0.x^{n-2}+n.x^{n-1}+0.x^n\end{aligned}$

Hence the required matrix is

$$\begin{pmatrix}0&1&0&0&\ldots&0\\0&0&2&0&\ldots&0\\0&0&0&3&&0\\\vdots&\vdots&\vdots&&&\vdots\\0&0&0&0&&n\\0&0&0&0&\ldots&0\end{pmatrix}$$

5. $T\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}x-y-z\\x+3y+z\\3x-y-2z\end{pmatrix}=\begin{pmatrix}1&-1&-1\\1&3&1\\3&-1&-2\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=A\underline{x}$

Range of T = span of the columns of A.

The columns of A have the same span as the rows of A^t and the rows of the following arrays:

$\begin{pmatrix}1&1&3\\-1&3&-1\\-1&1&-2\end{pmatrix}\begin{matrix}r_2\to r_2+r_1\\r_3\to r_3+r_1\end{matrix}\quad\begin{pmatrix}1&1&3\\0&4&2\\0&2&1\end{pmatrix}r_3\to 2r_3-r_2\quad\begin{pmatrix}1&1&3\\0&4&2\\0&0&0\end{pmatrix}$

Hence the span of the columns of A has basis $\left\{\begin{pmatrix}1\\1\\3\end{pmatrix},\begin{pmatrix}0\\2\\1\end{pmatrix}\right\}$ and so the range space of T has basis $\left\{\begin{pmatrix}1\\1\\3\end{pmatrix},\begin{pmatrix}0\\2\\1\end{pmatrix}\right\}$.

Now find a basis for the null space $N(T)$. $\begin{pmatrix}x\\y\\z\end{pmatrix}\in N(T)$ if and only if $A\begin{pmatrix}x\\y\\z\end{pmatrix}=\underline{0}$ i.e. if and

only if $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ is a solution of the systems represented by the following arrays:

$$\left(\begin{array}{ccc|c} 1 & -1 & -1 & 0 \\ 1 & 3 & 1 & 0 \\ 3 & -1 & -2 & 0 \end{array}\right) \begin{array}{l} r_2 \to r_2 - r_1 \\ r_3 \to r_3 - 3r_1 \end{array} \left(\begin{array}{ccc|c} 1 & -1 & -1 & 0 \\ 0 & 4 & 2 & 0 \\ 0 & 2 & 1 & 0 \end{array}\right) r_3 \to 2r_3 - r_2$$

$$\left(\begin{array}{ccc|c} 1 & -1 & -1 & 0 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) r_2 \to \frac{r_2}{2} \left(\begin{array}{ccc|c} 1 & -1 & -1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

i.e. $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in N(T)$ if and only if $\begin{array}{rcl} x-y-z & = & 0 \\ 2y+z & = & 0 \end{array}$

Let $z = \alpha$ then $y = -\frac{1}{2}\alpha$ and $x = \frac{1}{2}\alpha$. So $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \alpha \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 1 \end{pmatrix}$

Hence a basis for the kernel of T is $\left\{ \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} \right\}$.

6. $T(a_0+a_1x+a_2x^2) = a_0x+a_1x^2+a_2x^3$, so $R(T) = \{ax+bx^2+cx^3 \,|\, a,b,c \in \mathbb{R}\}$. The set $\{x, x^2, x^3\}$ spans $R(T)$ and is linearly independent so is a basis for $R(T)$. Thus T has rank 3.
$N(T) = \{a_0+a_1x+a_2x^2 \,|\, a_0x+a_1x^2+a_2x^3 = 0\} = \{0\}$. Hence the nullity of T is $\dim\{0\}$ which is 0.

7. (a) Define $T : \mathbb{R}^5 \to \mathbb{R}^3$ by $T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix}$

Then $R(T) = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} \in \mathbb{R}^3 \,|\, x_1, x_2 \in \mathbb{R} \right\}$. Thus $R(T)$ has basis $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$ so Rank$(T) = 2$. Hence the nullity of $T = 5 - \text{Rank}(T) = 3$

$N(T) = \left\{ \begin{pmatrix} 0 \\ 0 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \,|\, x_3, x_4, x_5 \in \mathbb{R} \right\}$ this has basis $\left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$.

(b) Define $T : M_{22} \to M_{22}$ by $T \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$.

Then $R(T) = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \,|\, a,b,c \in \mathbb{R} \right\}$. $R(T)$ has basis $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}$ and so Rank$(T) = 3$.
The nullity of $T = dim M_{22} - \text{Rank}(T) = 4 - 3 = 1$
$N(T) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \,|\, d \in \mathbb{R} \right\}$. A basis for $N(T)$ is $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

TEST - 4

1. Let $A = \begin{pmatrix} 1 & -1 & 2 & 1 \\ 2 & 1 & -1 & 2 \\ 2 & -1 & 3 & -1 \\ 1 & 1 & -2 & 4 \end{pmatrix}$

   (a) Find a basis for the row space of A. What is the rank of A ? Use the rank to determine the dimension of the set of solutions of the system of equations $A\underline{x} = \underline{0}$.

   (b) Find a basis for the set of solutions of $A\underline{x} = \underline{0}$ and observe that the dimension agrees with that predicted in (a).

2. Let $A = \begin{pmatrix} 1 & 2 & -1 & 4 \\ 2 & -1 & 3 & 3 \\ -1 & 3 & -4 & 1 \\ 0 & 1 & -1 & 1 \end{pmatrix}$

   Find bases for the row and column spaces of A.

3. Give examples of nonzero m x n matrices A such that

   (a) $\rho(A) = \min\{m,n\}$

   (b) $\rho(A) < \min\{m,n\}$

4. Prove that if A is a 3 x 5 matrix then the column vectors of A are linearly dependent.

5. Prove that if A is a matrix which is not square, then either the row vectors of A or the column vectors of A are linearly dependent.

6. Let A be a 3 x 4 matrix with $\rho(A) = 3$.

   (a) What is the dimension of $\{\underline{x} : A\underline{x} = \underline{0}\}$?

   (b) Is $A\underline{x} = \underline{b}$ consistent for all $\underline{b}$?

   (c) If $A\underline{x} = \underline{b}$ is consistent, how many solutions does it have ?

   If A is a 4 x 3 matrix with $\rho(A) = 3$, what are the answers to (a), (b) and (c) ?

Solutions

1. (a) The row space of A is the same as the row spaces of the following arrays:

$$\begin{pmatrix} 1 & -1 & 2 & 1 \\ 2 & 1 & -1 & 2 \\ 2 & -1 & 3 & -1 \\ 1 & 1 & -2 & 4 \end{pmatrix} \begin{matrix} r_2 \to r_2 - 2r_1 \\ r_3 \to r_3 - 2r_1 \\ r_4 \to r_4 - r_1 \end{matrix} \begin{pmatrix} 1 & -1 & 2 & 1 \\ 0 & 3 & -5 & 0 \\ 0 & 1 & -1 & -3 \\ 0 & 2 & -4 & 3 \end{pmatrix} \begin{matrix} r_3 \to 3r_3 - r_2 \\ r_4 \to 3r_4 - 2r_2 \end{matrix}$$

$$\begin{pmatrix} 1 & -1 & 2 & 1 \\ 0 & 3 & -5 & 0 \\ 0 & 0 & 2 & -9 \\ 0 & 0 & -2 & 9 \end{pmatrix} r_4 \to r_4 + r_3 \quad \begin{pmatrix} 1 & -1 & 2 & 1 \\ 0 & 3 & -5 & 0 \\ 0 & 0 & 2 & -9 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Hence the row space has basis $\{(1,-1,2,1),(0,3,-5,0),(0,0,2,-9)\}$ and thus the rank of A is $\mathrm{R}rank(A) = 3$. The solution space of the system $A\underline{x} = \underline{0}$ has dimension $4 - \mathrm{R}rank(A) = 4 - 3 = 1$.

(b) The system of equations $A\underline{x} = \underline{0}$ has the same solutions as the systems represented by:

$$\left(\begin{array}{cccc|c} 1 & -1 & 2 & 1 & 0 \\ 2 & 1 & -1 & 2 & 0 \\ 2 & -1 & 3 & -1 & 0 \\ 1 & 1 & -2 & 4 & 0 \end{array}\right)$$

Performing the same row operations as in (a) above we get:

$$\left(\begin{array}{cccc|c} 1 & -1 & 2 & 1 & 0 \\ 0 & 3 & -5 & 0 & 0 \\ 0 & 0 & 2 & -9 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

i.e. $A\underline{x} = \underline{0}$ has the same solutions as $\begin{aligned} x_1 - x_2 + 2x_3 + x_4 &= 0 \\ 3x_2 - 5x_3 &= 0 \\ 2x_3 - 9x_4 &= 0 \end{aligned}$

Let $x_4 = \alpha$. Then $x_3 = \frac{9}{2}\alpha$, $x_2 = \frac{15}{2}\alpha$, $x_1 = -\frac{5}{2}\alpha$

i.e. $\underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \frac{\alpha}{2}\begin{pmatrix} -5 \\ 15 \\ 9 \\ 2 \end{pmatrix}$

Thus $\left\{\begin{pmatrix} -5 \\ 15 \\ 9 \\ 2 \end{pmatrix}\right\}$ is a basis for the solution set $\{\underline{x} \in \mathbb{R}^4 \mid A\underline{x} = \underline{0}\}$ and so $\dim\{\underline{x} \mid A\underline{x} = \underline{0}\} = 1$ as predicted above.

2. The row space of A is the same as the row space of the following arrays:

$$\begin{pmatrix} 1 & 2 & -1 & 4 \\ 2 & -1 & 3 & 3 \\ -1 & 3 & -4 & 1 \\ 0 & 1 & -1 & 1 \end{pmatrix} \begin{matrix} r_2 \to r_2 - 2r_1 \\ r_3 \to r_3 + r_1 \end{matrix} \begin{pmatrix} 1 & 2 & -1 & 4 \\ 0 & -5 & 5 & -5 \\ 0 & 5 & -5 & 5 \\ 0 & 1 & -1 & 1 \end{pmatrix} \begin{matrix} r_3 \to r_3 + r_2 \\ r_4 \to 5r_4 + r_2 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & -1 & 4 \\ 0 & -5 & 5 & -5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} r_2 \to -\frac{1}{5}r_2 \quad \begin{pmatrix} 1 & 2 & -1 & 4 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Hence the row space has basis $\{(1,2,-1,4),(0,1,-1,1)\}$. To find a basis for the column space of A we could perform row operations on A^t or alternatively: notice that $\mathrm{R}rank(A) = 2$

(since the row space is two dimensional). Hence the column space has dimension 2 so any two linearly independent vectors in the column space will do. Since the first two columns of A, $(1,2,-1,0)$ and $(2,-1,3,1)$, are linearly independent (they are not multiples of each other) $\{(1,2,-1,0),(2,-1,3,1)\}$ is a basis for the column space.

3. (a) Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Then $m = n = 2$ and R$ank(A) = 2 = \min\{m,n\}$.

(b) Let $A = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$
Then $m = n = 2$ and R$ank(A) = 1 < \min\{m,n\}$

4. Let $A = (\underline{a}_1\ \underline{a}_2\ \underline{a}_3\ \underline{a}_4\ \underline{a}_5)$ where $\underline{a}_i$ $i = 1,2,\ldots,5$ are the columns of A. $\underline{a}_i \in \mathbb{R}^3$ each i so $\{\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_5\}$ is a set of 5 vectors in $\mathbb{R}^3$ so is linearly dependent.

5. Suppose that A is an $m \times n$ matrix. Since A is not square $m \neq n$ so either $m > n$ or $m < n$.

(a) If $m > n$ the rows are a set of m vectors in $\mathbb{R}^n$. There are more vectors than the dimension of the vector space to which they belong so the rows form a linearly dependent set.

(b) If $m < n$ the columns are a set of n vectors in $\mathbb{R}^m$ so they are linearly dependent.

Hence either the rows or the columns are dependent.

6. (a) $\dim\{\underline{x} \in \mathbb{R}^4 \mid A\underline{x} = \underline{0}\} = 4 - $ R$ank(A) = 4 - 3 = 1$.

(b) $A\underline{x} = \underline{b}$ is consistent if and only if $\underline{b}$ is in the column space of A. Since R$ank(A) = 3$ and the column space is a subspace of $\mathbb{R}^3$, the column space is $\mathbb{R}^3$.
Hence $A\underline{x} = \underline{b}$ is consistent for all $\underline{b} \in \mathbb{R}^3$.

(c) From (b) $A\underline{x} = \underline{b}$ has a solution $\underline{x}_1$. If $\underline{x}_0$ is any solution of $A\underline{x} = \underline{0}$ then $\underline{x}_1 + \underline{x}_0$ is a solution of $A\underline{x} = \underline{b}$. Since $A\underline{x} = \underline{0}$ has infinitely many solutions, $A\underline{x} = \underline{b}$ has infinitely many solutions.

Suppose now A is 4×3 with R$ank(A) = 3$.

(a) $\dim\{\underline{x} \in \mathbb{R}^3 \mid A\underline{x} = \underline{0}\} = 3 - $ R$ank(A) = 3 - 3 = 0$. So $\underline{x} = \underline{0}$ is the only solution.

(b) The column space is a subspace of $\mathbb{R}^4$. Since R$ank(A) = 3$ the column space has dimension 3 and so is not equal to $\mathbb{R}^4$. Hence there exists $\underline{b} \in \mathbb{R}^4$ such that $A\underline{x} = \underline{b}$ is inconsistent.

(c) Since $A\underline{x} = \underline{0}$ has unique solution $\underline{x} = \underline{0}$, it follows that if $A\underline{x} = \underline{b}$ is consistent it has only one solution. (Any two solutions of $A\underline{x} = \underline{b}$ differ by a solution of $A\underline{x} = \underline{0}$.)

TEST - 5

1. Determine if $(3,4,-1,6)$ lies in span$\{(1,2,-1,2),(-2,3,1,-1),(-1,3,2,1)\}$ in $\mathbb{R}^4$.

2. Determine whether the given set of vectors spans the given vector space

   (a) In $\mathbb{R}^3$: $(1,-1,2),(1,1,2),(0,0,1)$

   (b) In P_2: $1-x,3-x^2,x$

   (c) In M_{22}: $\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix},\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix},\begin{pmatrix} 3 & -1 \\ 0 & 0 \end{pmatrix},\begin{pmatrix} 0 & 0 \\ 3 & 1 \end{pmatrix}$.

3. Let V be a vector space and suppose u_1,u_2,u_3 span V.
   Let $v_1=u_1,v_2=u_2-u_1,v_3=u_3$. Prove that v_1,v_2,v_3 also span V.

4. Let V be a vector space and let $v\in V$. If v is a linear combination of the vectors $\{u_1,\ldots,u_n\}$ and if each u_i is a linear combination of the vectors $\{w_1,\ldots,w_m\}$, prove that v is a linear combination of $\{w_1,\ldots,w_m\}$.

5. Determine whether the vectors $(1,2,3),(1,-1,2),(1,-4,2)$ in $\mathbb{R}^3$ are linearly independent.

6. Show that the vectors $u_1=(0,3,1,-1)$, $u_2=(6,0,5,1)$ and $u_3=(4,-7,1,3)$ form a linearly dependent set in $\mathbb{R}^4$.
   Express each vector as a linear combination of the other two.

7. Determine a value for q such that the following vectors are linearly independent

   $$(1,1,2,1),(2,1,2,3),(1,4,2,1),(-1,3,5,q)$$

8. Let V be a vector space and suppose that u_1,u_2,u_3 are linearly independent vectors in V. Prove that u_1+u_2,u_2+u_3,u_3 are also linearly independent.

9. Let V be a vector space and let $u,v,w\in V$. Show that the vectors $u-v,v-w$ and $w-u$ are linearly dependent.

10. Let V be a vector space and let $S=\{u_1,\ldots,u_n\}\subseteq V$. If S_1 is a nonempty subset of S, prove or give counterexamples to the following statements.

    (a) If S spans V, then S_1 spans V.

    (b) If S is linearly independent, then S_1 is linearly independent.

    (c) If S_1 spans V, then S spans V.

    (d) If S_1 is linearly independent, then S is linearly independent.

Solutions

1. We seek c_1,c_2,c_3 such that $c_1\begin{pmatrix}1\\2\\-1\\2\end{pmatrix}+c_2\begin{pmatrix}-2\\3\\1\\-1\end{pmatrix}+c_3\begin{pmatrix}-1\\3\\2\\1\end{pmatrix}=\begin{pmatrix}3\\4\\-1\\6\end{pmatrix}$

i.e. we require
$$\begin{aligned} c_1-2c_2-c_3 &= 3\\ 2c_1+3c_2+3c_3 &= 4 \qquad (*)\\ -c_1+c_2+2c_3 &= -1\\ 2c_1-c_2+c_3 &= 6 \end{aligned}$$

Using Gaussian elimination:

$$\left(\begin{array}{ccc|c}1&-2&-1&3\\2&3&3&4\\-1&1&2&-1\\2&-1&1&6\end{array}\right)\begin{matrix}r_2\to r_2-2r_1\\ r_3\to r_3+r_1\\ r_4\to r_4-2r_1\end{matrix}\left(\begin{array}{ccc|c}1&-2&-1&3\\0&7&5&-2\\0&-1&1&2\\0&3&3&0\end{array}\right)\begin{matrix}r_3\to 7r_3+r_2\\ r_4\to 7r_4-3r_2\end{matrix}$$

$$\left(\begin{array}{ccc|c}1&-2&-1&3\\0&7&5&-2\\0&0&12&12\\0&0&6&6\end{array}\right)r_4\to 2r_4-r_3\left(\begin{array}{ccc|c}1&-2&-1&3\\0&7&5&-2\\0&0&12&12\\0&0&0&0\end{array}\right)r_3\to\frac{1}{12}r_3\left(\begin{array}{ccc|c}1&-2&-1&3\\0&7&5&-2\\0&0&1&1\\0&0&0&0\end{array}\right)$$

i.e. $(*)$ has the same solutions as
$$\begin{aligned} c_1-2c_2-c_3 &= 3\\ 7c_2+5c_3 &= -2\\ c_3 &= 1 \end{aligned}$$

So $c_3=1, c_2=-1, c_1=2$. Thus $\begin{pmatrix}3\\4\\-1\\6\end{pmatrix}=2\begin{pmatrix}1\\2\\-1\\2\end{pmatrix}-\begin{pmatrix}-2\\3\\1\\-1\end{pmatrix}+\begin{pmatrix}-1\\3\\2\\1\end{pmatrix}$

So $\begin{pmatrix}3\\4\\-1\\6\end{pmatrix}\in span\left\{\begin{pmatrix}1\\2\\-1\\2\end{pmatrix},\begin{pmatrix}-2\\3\\1\\-1\end{pmatrix},\begin{pmatrix}-1\\3\\2\\1\end{pmatrix}\right\}$

2. (a) Let $(x,y,z)\in\mathbb{R}^3$. We seek c_1,c_2,c_3 such that
$c_1(1,-1,2)+c_2(1,1,2)+c_3(0,0,1)=(x,y,z)$.
i.e. we require
$$\begin{aligned} c_1+c_2 &= x\\ -c_1+c_2 &= y\\ 2c_1+2c_2+c_3 &= z \end{aligned}$$
Using Gaussian elimination we have:
$$\left(\begin{array}{ccc|c}1&1&0&x\\-1&1&0&y\\2&2&1&z\end{array}\right)\begin{matrix}r_2\to r_2+r_1\\ r_3\to r_3-2r_1\end{matrix}\left(\begin{array}{ccc|c}1&1&0&x\\0&2&0&x+y\\0&0&1&z-2x\end{array}\right)$$
i.e.
$$\begin{aligned} c_1+c_2 &= x\\ 2c_2 &= x+y\\ c_3 &= z-2x \end{aligned}$$
So $c_3=z-2x$, $c_2=\frac{1}{2}(x+y)$, $c_1=\frac{1}{2}(x-y)$.
Thus $(x,y,z)=\frac{1}{2}(x-y)(1,-1,2)+\frac{1}{2}(x+y)(1,1,2)+(z-2x)(0,0,1)$.
Hence the given vectors span $\mathbb{R}^3$.

(b) Suppose $a_0+a_1x+a_2x^2\in P_2$. We seek c_1,c_2,c_3 such that
$$\begin{aligned} c_1(1-x)+c_2(3-x^2)+c_3x &= a_0+a_1x+a_2x^2\\ \text{i.e. } (c_1+3c_2)+(c_3-c_1)x-c_2x^2 &= a_0+a_1x+a_2x^2 \end{aligned}$$

i.e. $\begin{aligned} c_1+3c_2 &= a_0 \\ c_3-c_1 &= a_1 \\ -c_2 &= a_2 \end{aligned}$

So $c_2=-a_2$, $c_1=a_0+3a_2$, $c_3=a_1+a_0+3a_2$

Hence $a_0+a_1x+a_2x^2=(a_0+3a_2)(1-x)+(-a_2)(3-x^2)+(a_0+a_1+3a_2)x$

Hence $\{1-x,3-x^2,x\}$ span P_2.

(c) Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{22}$. We seek c_1,c_2,c_3,c_4 such that

$$c_1\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}+c_2\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix}+c_3\begin{pmatrix} 3 & -1 \\ 0 & 0 \end{pmatrix}+c_4\begin{pmatrix} 0 & 0 \\ 3 & 1 \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

i.e. $\begin{pmatrix} 2c_1+3c_3 & c_1-c_3 \\ 2c_2+3c_4 & c_2+c_4 \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Thus we require $\begin{aligned} 2c_1+3c_3 &= a \quad (1) \\ c_1-c_3 &= b \quad (2) \\ 2c_2+3c_4 &= c \quad (3) \\ c_2+c_4 &= d \quad (4) \end{aligned}$

$(1)-2\times(2)$ gives $5c_3=a-2b$ i.e. $c_3=\frac{1}{5}(a-2b)$ and then $c_1=b+c_3=\frac{1}{5}(a+3b)$. $(3)-2\times(4)$ gives $c_4=c-2d$ and then $c_2=d-c_4=3d-c$. Thus we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\frac{1}{5}(a+3b)\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}+(3d-c)\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix}+\frac{1}{5}(a-2b)\begin{pmatrix} 3 & -1 \\ 0 & 0 \end{pmatrix}+(c-2d)\begin{pmatrix} 0 & 0 \\ 3 & 1 \end{pmatrix}$$

Hence the given matrices span M_{22}.

3. Suppose $v\in V$. Since u_1,u_2,u_3 span V there exist constants c_1,c_2,c_3 such that $v=c_1u_1+c_2u_2+c_3u_3$.
But $u_1=v_1, u_2=v_1+v_2, u_3=v_3$
So $v=c_1v_1+c_2(v_1+v_2)+c_3v_3=(c_1+c_2)v_1+c_2v_2+c_3v_3$.
Hence v_1,v_2,v_3 span V.

4. Since v is a linear combination of $\{u_1,u_2,\ldots,u_n\}$ there exist $c_1,\ldots,c_n\in\mathbb{R}$ such that $v=c_1u_1+c_2u_2+\ldots+c_nu_n$.
Since each u_i is a linear combination of $\{w_1,\ldots,w_m\}$ there exist $d_{ij}\in\mathbb{R}$ $1\le i\le n$, $1\le j\le m$ such that $u_i=d_{i1}w_1+d_{i2}w_2+\ldots+d_{im}w_m$. Hence:

$$\begin{aligned} v &= c_1u_1+c_2u_2+\ldots+c_nu_n \\ &= c_1(d_{11}w_1+d_{12}w_2+\ldots+d_{1m}w_m) \\ &\quad +c_2(d_{21}w_1+d_{22}w_2+\ldots+d_{2m}w_m) \\ &\quad +\ldots \\ &\quad +c_n(d_{n1}w_1+d_{n2}w_2+\ldots+d_{nm}w_m) \\ &= (c_1d_{11}+c_2d_{21}+\ldots+c_nd_{n1})w_1 \\ &\quad +(c_1d_{12}+c_2d_{22}+\ldots+c_nd_{n2})w_2 \\ &\quad +\ldots \\ &\quad +(c_1d_{1m}+c_2d_{2m}+\ldots+c_nd_{nm})w_m \end{aligned}$$

i.e. v is a linear combination of $w_1,w_2,\ldots,w_m$ as required.
Alternatively, using Σ notation:

$$v = \sum_{i=1}^{n}c_iu_i = \sum_{i=1}^{n}c_i\Big(\sum_{j=1}^{m}d_{ij}w_j\Big) = \sum_{j=1}^{m}\Big(\sum_{i=1}^{n}c_id_{ij}\Big)w_j$$

5. Suppose that $c_1\begin{pmatrix}1\\2\\3\end{pmatrix}+c_2\begin{pmatrix}1\\-1\\2\end{pmatrix}+c_3\begin{pmatrix}1\\-4\\2\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$

Then $\begin{aligned} c_1+c_2+c_3 &= 0\\ 2c_1-c_2-4c_3 &= 0 \quad (*)\\ 3c_1+2c_2+2c_3 &= 0\end{aligned}$

Solutions of $(*)$ are the same as the solutions of the systems corresponding to:

$\left(\begin{array}{ccc|c}1&1&1&0\\2&-1&-4&0\\3&2&2&0\end{array}\right)$ $\begin{matrix}r_2\to r_2-2r_1\\ r_3\to r_3-3r_1\end{matrix}$ $\left(\begin{array}{ccc|c}1&1&1&0\\0&-3&-6&0\\0&-1&-1&0\end{array}\right)$ $r_2\to -\frac{1}{3}r_2$

$\left(\begin{array}{ccc|c}1&1&1&0\\0&1&2&0\\0&-1&-1&0\end{array}\right)$ $r_3\to r_3+r_2$ $\left(\begin{array}{ccc|c}1&1&1&0\\0&1&2&0\\0&0&1&0\end{array}\right)$

$\begin{aligned} c_1+c_2+c_3 &= 0\\ \text{i.e.}\quad c_2+2c_3 &= 0\\ c_3 &= 0\end{aligned}$

This has unique solution $c_1=c_2=c_3=0$ so the vectors are linearly independent.

6. Suppose that $c_1\begin{pmatrix}0\\3\\1\\-1\end{pmatrix}+c_2\begin{pmatrix}6\\0\\5\\1\end{pmatrix}+c_3\begin{pmatrix}4\\-7\\1\\3\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$

Then $\begin{aligned} 6c_2+4c_3 &= 0\\ 3c_1-7c_3 &= 0 \quad (*)\\ c_1+5c_2+c_3 &= 0\\ -c_1+c_2+3c_3 &= 0\end{aligned}$

$(*)$ has the same solutions as the systems corresponding to the following:

$\left(\begin{array}{ccc|c}0&6&4&0\\3&0&-7&0\\1&5&1&0\\-1&1&3&0\end{array}\right)$ $r_1\leftrightarrow r_3$ $\left(\begin{array}{ccc|c}1&5&1&0\\3&0&-7&0\\0&6&4&0\\-1&1&3&0\end{array}\right)$ $\begin{matrix}r_2\to r_2-3r_1\\ r_4\to r_4+r_1\end{matrix}$

$\left(\begin{array}{ccc|c}1&5&1&0\\0&-15&-10&0\\0&6&4&0\\0&6&4&0\end{array}\right)$ $\begin{matrix}r_3\to 5r_3+2r_2\\ r_4\to 5r_4+2r_2\end{matrix}$ $\left(\begin{array}{ccc|c}1&5&1&0\\0&-15&-10&0\\0&0&0&0\\0&0&0&0\end{array}\right)$ $r_2\to -\frac{1}{5}r_2$ $\left(\begin{array}{ccc|c}1&5&1&0\\0&3&2&0\\0&0&0&0\\0&0&0&0\end{array}\right)$

Thus we require $\begin{aligned} c_1+5c_2+c_3 &= 0\\ 3c_2+2c_3 &= 0\end{aligned}$

This has general solution $c_3=\alpha$, $c_2=-\frac{2}{3}\alpha$, $c_1=\frac{7}{3}\alpha$. Hence there are non-zero solutions and thus the vectors are linearly dependent. Taking $\alpha=3$ we obtain $7\begin{pmatrix}0\\3\\1\\-1\end{pmatrix}-2\begin{pmatrix}6\\0\\5\\1\end{pmatrix}+3\begin{pmatrix}4\\-7\\1\\3\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$ and so $\begin{pmatrix}0\\3\\1\\-1\end{pmatrix}=\frac{2}{7}\begin{pmatrix}6\\0\\5\\1\end{pmatrix}-\frac{3}{7}\begin{pmatrix}4\\-7\\1\\3\end{pmatrix}$; $\begin{pmatrix}6\\0\\5\\1\end{pmatrix}=\frac{7}{2}\begin{pmatrix}0\\3\\1\\-1\end{pmatrix}+\frac{3}{2}\begin{pmatrix}4\\-7\\1\\3\end{pmatrix}$; $\begin{pmatrix}4\\-7\\1\\3\end{pmatrix}=$

$$-\frac{7}{3}\begin{pmatrix}0\\3\\1\\-1\end{pmatrix}+\frac{2}{3}\begin{pmatrix}6\\0\\5\\1\end{pmatrix}.$$

7. Suppose $c_1\begin{pmatrix}1\\1\\2\\1\end{pmatrix}+c_2\begin{pmatrix}2\\1\\2\\3\end{pmatrix}+c_3\begin{pmatrix}1\\4\\2\\1\end{pmatrix}+c_4\begin{pmatrix}-1\\3\\5\\q\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$ $(*)$

c_1,c_2,c_3,c_4 satisfy $(*)$ if and only if
$$\begin{aligned} c_1+2c_2+c_3-c_4 &= 0\\ c_1+c_2+4c_3+3c_4 &= 0\\ 2c_1+2c_2+2c_3+5c_4 &= 0\\ c_1+3c_2+c_3+qc_4 &= 0\end{aligned}$$
So $(*)$ has the same solutions as the systems represented by
$$\left(\begin{array}{cccc|c}1&2&1&-1&0\\1&1&4&3&0\\2&2&2&5&0\\1&3&1&q&0\end{array}\right)\begin{array}{l}r_2\to r_2-r_1\\r_3\to r_3-2r_1\\r_4\to r_4-r_1\end{array}\left(\begin{array}{cccc|c}1&2&1&-1&0\\0&-1&3&4&0\\0&-2&0&7&0\\0&1&0&q+1&0\end{array}\right)\begin{array}{l}r_3\to r_3-2r_2\\r_4\to r_4+r_2\end{array}$$
$$\left(\begin{array}{cccc|c}1&2&1&-1&0\\0&-1&3&4&0\\0&0&-6&-1&0\\0&0&3&q+5&0\end{array}\right)r_4\to 2r_4+r_3\left(\begin{array}{cccc|c}1&2&1&-1&0\\0&-1&3&4&0\\0&0&-6&-1&0\\0&0&0&2q+9&0\end{array}\right)$$
The system has the unique solution $c_1=c_2=c_3=c_4=0$ if and only if $2q+9\neq 0$. Hence the vectors are linearly independent iff $2q+9\neq 0$. Thus $q=1$, for example, yields a linearly independent set of vectors.

8. Suppose that $c_1(u_1+u_2)+c_2(u_2+u_3)+c_3u_3 = \underline{0}$
Then $c_1u_1+(c_1+c_2)u_2+(c_2+c_3)u_3 = \underline{0}$
Hence, since u_1,u_2,u_3 are linearly independent, $c_1=0$, $c_1+c_2=0$ and $c_2+c_3=0$. Now $c_1=0\Rightarrow c_2=0$ $\Rightarrow c_3=0$ and hence u_1+u_2,u_2+u_3,u_3 are linearly independent.

9. $(u-v)+(v-w)+(w-u)=\underline{0}$
So $u-v,v-w,w-u$ are linearly dependent.

10. (a) False. Let $V=\mathbb{R}^2$, $S=\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$, and $S_1=\left\{\begin{pmatrix}1\\0\end{pmatrix}\right\}$.
Then S spans V, but S_1 does not span V.

(b) True. Suppose, reordering the vectors if necessary, that $S_1=\{u_1,u_2,\ldots,u_k\}$ where $k\leq n$. We shall show that S_1 is a linearly independent set of vectors. Suppose $c_1u_1+c_2u_2+\ldots+c_ku_k=\underline{0}$. Then $c_1u_1+c_2u_2+\ldots+c_ku_k+0u_{k+1}+0u_{k+2}+\ldots+0u_n=\underline{0}$. Since $u_1,u_2,\ldots,u_n$ are linearly independent this implies that $c_1=c_2=\ldots=c_k=0$. Hence $u_1,u_2,\ldots,u_k$ are linearly independent.

(c) True. Suppose $S_1=\{u_1,u_2,\ldots,u_k\}$ (renumbering if necessary) and that S_1 spans V. We shall show that S spans V: Take $v\in V$. Since S_1 spans V, $\exists\, c_1,c_2,\ldots,c_k$ that $v=c_1u_1+c_2u_2+\ldots+c_ku_k$ so $v=c_1u_1+c_2u_2+\ldots+c_ku_k+0u_{k+1}+0u_{k+2}+\ldots+0u_n$ i.e. v is a linear combination of $u_1,u_2,\ldots,u_n$. Hence $u_1,u_2,\ldots,u_n$ span V.

(d) False. Let $V=\mathbb{R}^2$, $S=\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\}$ and $S_1=\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$. Then S_1 is linearly independent, but S is linearly dependent as
$$\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}-\begin{pmatrix}1\\1\end{pmatrix}=0.$$

TEST - 6

1. Show that:
   (a) The set of vectors of the form $(a,0,0)$ is a subspace of $\mathbb{R}^3$;
   (b) The set of vectors of the form $(a,1,0)$ is not a subspace of $\mathbb{R}^3$;
   (c) The set of vectors of the form $(a,3a,2a)$ is a subspace of $\mathbb{R}^3$;
   (d) $\{(x,y,z)\,|\,x^2+y^2+z^2 \leq 1\}$ is not a subspace of $\mathbb{R}^3$.

2. Determine which of the following are subspaces of M_{22}:
   (a) The set of matrices of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a,b,c and d are integers;
   (b) The set of 2 x 2 matrices such that $A = A^t$ where t denotes matrix transpose;
   (c) The set of 2 x 2 matrices such that $det(A) = 0$.

3. Determine which of the following are subspaces of P_3, the space of all polynomials of degree 3 or less:
   (a) The set of polynomials $a_0 + a_1x + a_2x^2 + a_3x^3$ for which $a_0 = 0$;
   (b) The set of polynomials $a_0 + a_1x + a_2x^2 + a_3x^3$ for which $a_0 + a_1 + a_2 + a_3 = 0$.

4. Determine which of the following are subspaces of V, the vector space of all real valued functions defined on $\mathbb{R}$:
   (a) The family of all f's such that $f(0) = 0$;
   (b) The family of all f's such that $f(0) = 1$;
   (c) The family of all continuous functions f;
   (d) The family of all differentiable functions f.

5. Let $(V,+,.)$ be a vector space. Let $\underline{0}$ denote the zero vector and let $-u$ denote the additive inverse of u. Prove that
   (a) $0.u = \underline{0}$ for all $u \in V$.
   (b) $\alpha.(-u) = -(\alpha.u)$ for all $u \in V$ and $\alpha \in \mathbb{R}$.
   (c) If $\alpha.u = \alpha.v$ where $\alpha \in \mathbb{R} - \{0\}$ and $u,v \in V$, then $u = v$.

Solutions

1. (a) Let $S=\{(a,0,0)\in\mathbb{R}^3\,|\,a\in\mathbb{R}\}$.
Suppose $u,v\in S$ and $\alpha\in\mathbb{R}$.
Then $u=(a_1,0,0)$ and $v=(a_2,0,0)$ for some $a_1,a_2\in\mathbb{R}$.
Now $u+v=(a_1,0,0)+(a_2,0,0)=(a_1+a_2,0,0)\in S$
and $\alpha u=\alpha(a_1,0,0)=(\alpha a_1,0,0)\in S$.
Hence S is a subspace of $\mathbb{R}^3$.

(b) Let $S=\{(a,1,0)\in\mathbb{R}^3\,|\,a\in\mathbb{R}\}$.
$\underline{0}=(0,0,0)\notin S$, so S is not a subspace of $\mathbb{R}^3$.

(c) Let $S=\{(a,3a,2a)\in\mathbb{R}^3\,|\,a\in\mathbb{R}\}$.
Suppose $u,v\in S$ and $\alpha\in\mathbb{R}$.
Then $u=(a_1,3a_1,2a_1)$ and $v=(a_2,3a_2,2a_2)$ for some $a_1,a_2\in\mathbb{R}$.
Now $\begin{aligned} u+v=(a_1,3a_1,2a_1)+(a_2,3a_2,2a_2) &= (a_1+a_2,3a_1+3a_2,2a_1+2a_2)\\ &= (a_1+a_2,3(a_1+a_2),2(a_1+a_2))\\ &\in S\end{aligned}$
and $\alpha u=\alpha(a_1,3a_1,2a_1)=(\alpha a_1,\alpha 3a_1,\alpha 2a_1)=(\alpha a_1,3(\alpha a_1),2(\alpha a_1))\in S$.
Hence S is a subspace of $\mathbb{R}^3$.

(d) Let $S=\{(x,y,z)\in\mathbb{R}^3\,|\,x^2+y^2+z^2\le 1,x,y,z\in\mathbb{R}\}$.
Take $u=(1,0,0)$ and $v=(0,1,0)$. Now $u,v\in S$
but $u+v=(1,0,0)+(0,1,0)=(1,1,0)$ and $1^2+1^2+0^2=2$ so $u+v\notin S$.
Hence S is not a subspace of $\mathbb{R}^3$.

2. (a) Let $S=\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_{22}\,|\,a,b,c,d\in\mathbb{Z}\}$.
Then $\begin{pmatrix}1&1\\1&1\end{pmatrix}\in S$ but $\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}=\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&\frac{1}{2}\end{pmatrix}\notin S$.
Hence S is not a subspace of M_{22}.

(b) Let $S=\{A\in M_{22}\,|\,A=A^t\}$.
Suppose $A,B\in S$ and $\alpha\in\mathbb{R}$.
Then $\begin{aligned}(A+B)^t &= A^t+B^t \quad \text{(property of matrix transpose)}\\ &= A+B \quad (\text{since } A,B\in S)\end{aligned}$
so $A+B\in S$
Also $(\alpha A)^t=\alpha A^t=\alpha A$, so $\alpha A\in S$.
Hence S is a subspace of M_{22}.

(c) Let $S=\{A\in M_{22}\,|\,detA=0\}$.
Let $A=\begin{pmatrix}1&0\\0&0\end{pmatrix},B=\begin{pmatrix}0&0\\0&1\end{pmatrix}$, then $A+B=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

Now $detA = detB = 0$, but $det(A+B) = 1$.
Hence $A, B \in S$, but $A+B \notin S$.
Hence S is not a subspace of M_{22}.

3. (a) Let $S = \{a_1x + a_2x^2 + a_3x^3 \mid a_1, a_2, a_3 \in \mathbb{R}\}$.
Suppose $p(x), q(x) \in S$ and $\alpha \in \mathbb{R}$.
Then $p(x) = a_1x + a_2x^2 + a_3x^3$ and $q(x) = b_1x + b_2x^2 + b_3x^3$ for some $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$.

$$\begin{aligned} \text{Now, } p(x)+q(x) &= (a_1x + a_2x^2 + a_3x^3) + (b_1x + b_2x^2 + b_3x^3) \\ &= (a_1+b_1)x + (a_2+b_2)x^2 + (a_3+b_3)x^3 \\ &\in S. \end{aligned}$$

$$\begin{aligned} \text{Also, } \alpha p(x) &= \alpha(a_1x + a_2x^2 + a_3x^3) \\ &= \alpha a_1x + \alpha a_2x^2 + \alpha a_3x^3 \\ &\in S. \end{aligned}$$

Hence S is a subspace of P_3.

(b) Let $S = \{a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{R},\ a_0 + a_1 + a_2 + a_3 = 0\}$.
Suppose $p(x), q(x) \in S$ and $\alpha \in \mathbb{R}$.
There exist $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3$ such that

$$\begin{aligned} p(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 \quad \text{where} \quad a_0 + a_1 + a_2 + a_3 = 0 \\ q(x) &= b_0 + b_1x + b_2x^2 + b_3x^3 \qquad\qquad\ \ b_0 + b_1 + b_2 + b_3 = 0 \end{aligned}$$

$$\begin{aligned} \text{Then } p(x)+q(x) &= (a_0 + a_1x + a_2x^2 + a_3x^3) + (b_0 + b_1x + b_2x^2 + b_3x^3) \\ &= (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + (a_3+b_3)x^3 \end{aligned}$$

Now,

$$\begin{aligned} (a_0+b_0) + (a_1+b_1) + (a_2+b_2) + (a_3+b_3) &= a_0 + a_1 + a_2 + a_3 + b_0 + b_1 + b_2 + b_3 \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

So $p+q \in S$.

$$\begin{aligned} \text{Also } \alpha p(x) &= \alpha(a_0 + a_1x + a_2x^2 + a_3x^3) \\ &= \alpha a_0 + \alpha a_1x + \alpha a_2x^2 + \alpha a_3x^3 \end{aligned}$$

$$\begin{aligned} \text{Now, } \alpha a_0 + \alpha a_1 + \alpha a_2 + \alpha a_3 &= \alpha(a_0 + a_1 + a_2 + a_3) \\ &= 0 \end{aligned}$$

so $\alpha p \in S$. Hence S is a subspace of P_3.

4. (a) Let $S = \{f \in V \mid f(0) = 0\}$.
Suppose $f, g \in S$ and $\alpha \in \mathbb{R}$.

$$\begin{aligned} \text{Then } (f+g)(0) &= f(0) + g(0) \\ &= 0 + 0 \qquad (\text{since } f, g \in S) \\ &= 0 \end{aligned}$$

So $f+g \in S$.
Also $(\alpha f)(0) = \alpha f(0) = 0$ (since $f \in S$) so $\alpha f \in S$.
Hence S is a subspace of V.

(b) Let $S = \{f \in V \mid f(0) = 1\}$.
Take $f(x) = 1 + x$ and $g(x) = 1 + x^2$. Now $f(0) = g(0) = 1$ so $f, g \in S$, but $(f+g)(0) = f(0) + g(0) = 2$. Hence $f+g \notin S$ and therefore S is not a subspace of V

(c) Let $S = \{f \in V \mid f \text{ is continuous}\}$
Suppose $f, g \in S$ and $\alpha \in \mathbb{R}$.
Then, as was discussed in the first year calculus course, $f+g$ and αf are continuous and so lie in S. Hence S is a subspace of V.

(d) Let $S = \{f \in V \mid f \text{ is differentiable}\}$.
Suppose $f, g \in S$ and $\alpha \in \mathbb{R}$.
As was shown in the the first year calculus course $f+g$ and αf are differentiable and so lie in S. Hence S is a subspace of V.

5. (a) $\begin{aligned} 0.u + 0.u &= (0+0).u \\ &= 0.u \\ &= 0.u + \underline{0} \end{aligned}$
Hence $0.u = \underline{0}$.

(b) $\begin{aligned} \alpha(-u) + \alpha u &= \alpha((-u)+u) \\ &= \alpha\underline{0} \\ &= \underline{0} \end{aligned}$
Hence $\alpha(-u) = -\alpha u$.

(c)
Suppose	αu	$=$	αv	$(\alpha \neq 0)$
Then	$\frac{1}{\alpha}(\alpha u)$	$=$	$\frac{1}{\alpha}(\alpha v)$	
so	$(\frac{1}{\alpha}\alpha)u$	$=$	$(\frac{1}{\alpha}\alpha)v$	(vector space axiom)
hence	$1u$	$=$	$1v$	
and so	u	$=$	v	(axiom)

TEST - 7

1. Abelian Groups

Problem 1.1 (Linear Algebra of Abelian Groups, Part I)**.** Let A be an abelian group, and suppose that $\{a_1, \ldots, a_n\} \in A$ is a generating set for A.

(1) Show that for $i \neq j$ and $k \in \mathbb{Z}$, the set $\{a_1, \ldots, a_{i-1}, a_i + ka_j, a_{i+1}, \ldots, a_n\}$ is also a generating set for A. Show moreover that this set is a basis for A if and only if $\{a_1, \ldots, a_n\}$ is.

(2) Show that for all i, the set $\{a_1, \ldots, a_{i-1}, (-a_i), a_{i+1}, \ldots, a_n\}$ is a generating set for A. Show moreover that this set is a basis if and only if $\{a_1, \ldots, a_n\}$ is.

Solution 1.1.1 (Solution to Part (1))**.** Let $x \in A$ be any element. Then there exist integers $m_i, \ldots, m_n$ such that

$$x = m_1 a_1 + \cdots + m_n a_n$$

since $a_1, \ldots, a_n$ is a generating set for A. Now, since $a_i = (a_i + ka_j) - ka_j$, we have $m_i a_i = m_i(a_i + ka_j) - m_i k a_j$, so

$$x = m_1 a_1 + \cdots + m_i(a_i + ka_j) + \cdots + (m_j - m_i k)a_j + \cdots + m_n a_n.$$

Hence $\{a_1, \ldots, a_{i-1}, a_i + ka_j, a_{i+1}, \ldots, a_n\}$ is also a generating set for A.

Suppose now that $\{a_1, \ldots, a_n\}$ is linearly independent. Suppose that

$$m_1 a_1 + \cdots + m_i(a_i + ka_j) + \cdots + m_n a_n = 0$$

for some $m_1, \ldots, m_n \in \mathbb{Z}$. We want to show that $m_\ell = 0$ for all ℓ. Expanding the above expression, we get

$$m_1 a_1 + \cdots + m_i a_i + \cdots + (m_j + m_i k)a_j + \cdots + m_n a_n = 0.$$

Since $a_1, \ldots, a_n$ are linearly independent, we have that $m_\ell = 0$ for all $\ell \neq j$, and $m_j + m_i k = 0$. But then in particular $m_i = 0$, so $0 = m_j + m_i k = m_j + 0$, so $m_j = 0$ also. Hence all the m_ℓ are 0, so $\{a_1, \ldots, a_{i-1}, a_i + ka_j, a_{i+1}, \ldots, a_n\}$ are linearly independent, hence a basis of A.

Solution 1.1.2 (Solution to Part (2))**.** This is easier. Let $x \in A$ be any element. Then there exist integers $m_i, \ldots, m_n$ such that

$$x = m_1 a_1 + \cdots + m_n a_n$$

since $a_1, \ldots, a_n$ is a generating set for A. Then

$$x = m_1 a_1 + \cdots + (-m_i)(-a_i) + \cdots + m_n a_n,$$

hence $\{a_1, \ldots, a_{i-1}, (-a_i), a_{i+1}, \ldots, a_n\}$ is a generating set for A.

Suppose now that $\{a_1, \ldots, a_n\}$ is linearly independent. Suppose that

$$m_1 a_1 + \cdots + m_i(-a_i) + \cdots + m_n a_n = 0$$

for some $m_1, \ldots, m_n \in \mathbb{Z}$. Then also

$$m_1 a_1 + \cdots + (-m_i) a_i + \cdots + m_n a_n = 0.$$

Since $a_1, \ldots, a_n$ are linearly independent, $m_j = 0$ for all $j \neq i$, and $-m_i = 0$. Hence also $m_i = 0$, and so $\{a_1, \ldots, a_{i-1}, (-a_i), a_{i+1}, \ldots, a_n\}$ is a linearly independent set, hence a basis for A.

Problem 1.2 (Linear Algebra of Abelian Groups, Part II)**. You are NOT required to write up this problem to submit. However, you must understand it completely, as you will need it for the next problem, and for the final exam, hint hint.**
Let H be a subgroup of $\mathbb{Z}^n$. We know that H is finitely generated; suppose $h_1, \ldots, h_k$ generate H. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{Z}^n$. We know that we can write each h_i as

$$h_i = (a_{1i}, a_{2i}, \ldots, a_{ni}) = \sum_{j=1}^{n} a_{ji} e_j.$$

Bundle this information as an $n \times k$-matrix $M = (a_{ij})$, so the ith column of M contains the coordinates of h_i.

(1) Show that exchanging the generators h_i and h_j corresponds to exchanging the ith and jth columns of M.
(2) Show that exchanging the basis vectors e_i and e_j corresponds to exchanging the ith and jth rows of M.
(3) Show that multiplying the generator h_i by -1 corresponds to multiplying the ith column of M by -1.
(4) Show that multiplying the basis vector e_i by -1 corresponds to multiplying the ith row of M by -1.
(5) For $i \neq j$ and $k \in \mathbb{Z}$, show that replacing the generator h_i by $h_i + k h_j$ corresponds to adding k times the jth column of M to the ith column of M.
(6) For $i \neq j$ and $k \in \mathbb{Z}$, show that replacing the basis vector e_i by $e_i + k e_j$ corresponds to *subtracting* k times the ith row of M from the jth row of M (note that the roles of i and j have also changed!).

Conclude that when calculating $\mathbb{Z}^n/H$, we may apply any of the above "elementary row and column operations" to M and obtain the same quotient.

Solution 1.2.1. The most confusing part is number (6), so let's explain that one. Let $e_1, \ldots, e_n$ be our current basis of $\mathbb{Z}^n$, and take some generator $x = a_1 e_1 + \cdots + a_n e_n$ of H. As a column vector, we express this element as

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Now, suppose we replace e_i by $e_i + ke_j$. Then, as in part 1 of problem 1, we have $e_i = (e_i + ke_j) - ke_j$, hence

$$x = a_1e_1 + \cdots + a_i(e_i + ke_j) + \cdots + (a_j - ka_i)e_j + \cdots + a_ne_n.$$

So the coordinates of x with respect to the new basis are $(a_1, \ldots, a_i, \ldots, a_j - ka_i, \ldots, a_n)$, i.e. we have replaced our original column vector by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j - ka_i \\ \vdots \\ a_n \end{pmatrix}.$$

In other words, we have subtracted k times the ith row of our vector from the jth row of our vector.

Problem 1.3 (Linear Algebra of Abelian Groups, Part III)**.** Let's use the previous problem to actually do some calculations!

(1) Let H be the subgroup of $\mathbb{Z}^2$ generated by $(6, 9)$. Use the previous problem to show that $\mathbb{Z}^2/H \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. By keeping track of the row operations you do, explain how to choose the basis of $\mathbb{Z}^2$ that gives this isomorphism.
(2) Let H be the subgroup of $\mathbb{Z}^3$ generated by $(1, 2, 3)$ and $(2, 2, 2)$. Calculate $\mathbb{Z}^3/H$ as a product of cyclic groups.
(3) Let H be the subgroup of $\mathbb{Z}^3$ generated by $\{(1, 2, 3), (3, 4, 5), (5, 6, 7), (7, 8, 9)\}$. Calculate $\mathbb{Z}^3/H$ as a product of cyclic groups.

Solution 1.3.1 (Solution to Part (1))**.** Using elementary row operations, we have

$$\begin{pmatrix} 6 \\ 9 \end{pmatrix} \sim \begin{pmatrix} 6 \\ 3 \end{pmatrix} \sim \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

Now, let e_1, e_2 be the original (standard) basis of $\mathbb{Z}^2$. From part (6) of the last problem, subtracting k times row i from row j corresponds to adding k times e_j to e_i. So, our first row operation is to subtract 1 times row 1 of our matrix from row 2 of our matrix; this corresponds to replacing e_1 by $e_1 + e_2$, so our new basis after the first row operation is $\{e_1 + e_2, e_2\}$. Now, our second row operation is to subtract 2 times row 2 from row 1, of our matrix, so we replace e_2 by $e_2 + 2(e_1 + e_2) = 2e_1 + 3e_2$. So the final basis we end up with is $\{e_1 + e_2, 2e_1 + 3e_2\}$, i.e. $\{(1, 1), (2, 3)\}$.

Now, with respect to this new basis, H is the subgroup of $\mathbb{Z}^2$ generated by $(0, 3)$, i.e. $H = \{0\} \times 3\mathbb{Z}$. Hence

$$\mathbb{Z}^2/H \cong \frac{\mathbb{Z} \times \mathbb{Z}}{\{0\} \times 3\mathbb{Z}} \cong \mathbb{Z}/\{0\} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Solution 1.3.2 (Solution to Part (2))**.** Applying elementary row and column operations to the matrix of generators gives:

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \\ 3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 2 & -2 \\ 3 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 2 & 2 \\ 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}.$$

Hence there is a basis of $\mathbb{Z}^3$ such that with respect to this basis, H is the subgroup generated by $(1,0,0)$ and $(0,2,0)$, i.e. $H = \mathbb{Z} \times 2\mathbb{Z} \times \{0\}$. Then

$$\mathbb{Z}^3/H \cong \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times 2\mathbb{Z} \times \{0\}} \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/\{0\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Solution 1.3.3 (Solution to Part (3))**.** Applying elementary row and column operations to the matrix of generators gives:

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 5 & 7 & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 & 6 \\ 2 & 2 & 4 & 6 \\ 3 & 2 & 4 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 3 & 2 & 0 & 0 \end{pmatrix}.$$

By part (2) we already know this matrix can be reduced to

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

using elementary row and column operations. Hence, as in part (2), there is a basis of $\mathbb{Z}^3$ such that with respect to this basis, H is the subgroup generated by $(1,0,0)$ and $(0,2,0)$, and again

$$\mathbb{Z}^3/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Problem 1.4. Let A and B be finitely generated abelian groups. Show that $\text{rank}(A \times B) = \text{rank}(A) + \text{rank}(B)$. (Hint: use the structure theorem, plus the proposition proved on the last homework that $\text{rank}(A) = \text{rank}(A/T(A))$.)

Solution 1.4.1. Let A and B be finitely generated abelian groups. By the structure theorem, we can write

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \mathbb{Z}^r$$

and

$$B \cong \mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_m\mathbb{Z} \times \mathbb{Z}^s$$

for some natural numbers $a_1, \ldots, a_n, b_1, \ldots, b_m, r$, and s. We then have

$$T(A) = \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \{0\},$$

so

$$A/T(A) \cong \frac{\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \mathbb{Z}^r}{\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \times \{0\}} \cong \mathbb{Z}^r.$$

Likewise $B/T(B) \cong \mathbb{Z}^s$. Thus we have $\text{rank}(A) = \text{rank}(A/T(A)) = \text{rank}(\mathbb{Z}^r) =$ r and likewise $\text{rank}(B) = s$.

Now, we have $T(A \times B) = T(A) \times T(B)$, so

$$\frac{A \times B}{T(A \times B)} = \frac{A \times B}{T(A) \times T(B)} \cong A/T(A) \times B/T(B) \cong \mathbb{Z}^r \times \mathbb{Z}^s = \mathbb{Z}^{r+s},$$

hence

$$\text{rank}(A \times B) = \text{rank}(A \times B/T(A \times B)) = \text{rank}(\mathbb{Z}^{r+s}) = r+s = \text{rank}(A)+\text{rank}(B).$$

2. Group Actions

Problem 2.1. Let $G = (\mathbb{R}, +)$, and define an action of G on $\mathbb{R}^2$ by letting $\theta \in G$ act by clockwise rotation by θ. Show that this is in fact an action of G. Find the orbits of this action (a geometric description will suffice), and for each $v \in \mathbb{R}^2$, compute the stabilizer of v.

Solution 2.1.1. Let $\theta_1, \theta_2 \in \mathbb{R}$ and $v \in \mathbb{R}^2$ be arbitrary. Then $(\theta_1 + \theta_2) \cdot (v)$ is v rotated by the angle $\theta_1 + \theta_2$. This is the same as rotating v by θ_1, then by θ_2, i.e.

$$(\theta_1 + \theta_2) \cdot v = \theta_2 \cdot (\theta_1 \cdot v)).$$

(Note the order here is unimportant since $\mathbb{R}$ is abelian). We also have to check that the identity of $\mathbb{R}$ acts trivially. But $0 \cdot v$ is v rotated by 0 radians, which is of course just v.

Let $v = (x, y) \in \mathbb{R}^2$ be arbitrary. Let $r = \sqrt{x^2 + y^2}$ be the length of v. Then the orbit of v consists of the circle of radius r; two vectors $v_1, v_2 \in \mathbb{R}^2$ differ by a rotation if and only if they have the same length. In the case $r = 0$, the orbit of $v = (0, 0)$ is just the single point v.

Now, suppose $v \in \mathbb{R}^2$ is a nonzero vector. Then $\theta \cdot v = v$ if and only if rotation by θ leaves v unchanged, which occurs only when θ is an integer multiple of 2π, i.e. the stabilizer G_v of v is $2\pi\mathbb{Z}$. On the other hand, if $v = (0, 0)$, then v is fixed by every rotation, so in this case $G_v = G$.

Problem 2.2 (Creative Problem: Properties of Group Actions)**.** Let G be a group and let X be a G-set.

(1) The action of G on X is called *faithful* if the only element of G which acts trivially is the identity, i.e. if for every $g \in G$, $g \cdot x = x$ for all $x \in X$ only if $g = e$. Give three examples of faithful group actions and three examples of non-faithful group actions.

(2) The action of G on X is called *transitive* if it has a single orbit, i.e. if for every $x, y \in X$ there is a $g \in G$ such that $g \cdot x = y$. Give three examples of transitive group actions and three examples of non-transitive group actions.

(3) Suppose that the action of G on X is both faithful and transitive and suppose that X is non-empty. Show that there is a bijection from G to X.

Solution 2.2.1 (Solution to Part (1))**.** Some faithful group actions:

(1) If G is any group, the left regular representation of G is a faithful action; if $g \cdot e = e$ then $ge = e$, so $g = e$.
(2) S_n acts faithfully on the set $\{1, \ldots, n\}$, since the only permutation which does not move any element is the identity. More generally, if X is any set, S_X acts faithfully on X.
(3) D_n acts faithfully on the vertices of the n-gon.
(4) The group $GL_2(\mathbb{R})$ acts faithfully on $\mathbb{R}^2$ by matrix multiplication. If $M \in GL_2(\mathbb{R})$ and

$$M \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$M \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

then M is the identity matrix.

Some non-faithful group actions:

(1) Let G be any nontrivial group. Then the trivial action of G on the one-element set $\{1\}$ is not faithful.
(2) Let $\mathbb{Z}$ act on $\mathbb{Z}/n\mathbb{Z}$ by $a + [b] = [a + b]$. This action is not faithful since every element in $n\mathbb{Z}$ fixes every element of $\mathbb{Z}/n\mathbb{Z}$.
(3) As in the previous problem, $(\mathbb{R}, +)$ acts on the plane by rotations; this action is not faithful since $2\pi\mathbb{Z} \subseteq \mathbb{R}$ fixes every element of $\mathbb{R}^2$.

Solution 2.2.2 (Solution to Part (2))**.** Some examples of transitive group actions:

(1) If G is any group, the left regular representation of G is transitive; let $g, h \in G$ be arbitrary. Then $(hg^{-1}) \cdot g = h$.
(2) The action of S_n on the set $\{1, \ldots, n\}$ is transitive.
(3) The action of D_n on the vertices of the $n - gon$ is transitive.
(4) If G is any group, the trivial action of G on the one-element set is transitive.
(5) The action of $\mathbb{Z}$ on $\mathbb{Z}/n\mathbb{Z}$ by $a + [b] = [a + b]$ is transitive, since if $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ are arbitrary then $[a] = (a - b) + [b]$.
(6) More generally, if G is any group and H is any subgroup of G, the action of G on the left cosets of H is transitive.

Some examples of non-transitive group actions:

(1) The action of $GL_2(\mathbb{R})$ on $\mathbb{R}^2$ is not transitive. There is no matrix $M \in GL_2(\mathbb{R})$ such that

$$M \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

(2) The actions of $(\mathbb{R}, +)$ on the plane by rotations is not transitive. Given $v_1, v_2 \in \mathbb{R}^2$, there is a $\theta \in \mathbb{R}$ such that $v_1 = \theta \cdot v_2$ if and only if v_1 and v_2 have the same length.

(3) Let S_3 act on the set $\{1,2,3\} \times \{1,2,3\}$ by $\sigma \cdot (a,b) = (\sigma(a), \sigma(b))$. This action is not transitive; for example, there is no σ such that $(1,2) = \sigma \cdot (1,1)$ since $\sigma \cdot (1,1)$ must have equal first and second coordinates.

(4) Let X be any set with 2 or more elements, let G be any group, and let G act on X trivially by $g \cdot x = x$ for all $x \in X$. Then this is not a transitive action.

Solution 2.2.3 (Solution to Part (3))**.** Part (3) is false. A counterexample is given by the usual action of S_3 on $\{1,2,3\}$. This is a faithful, transitive action, but $\{1,2,3\}$ has 3 elements whereas S_3 has 6.

The right condition to ask is that the action of G on X be *free*: this means that for all $x \in X$ and for all $g, h \in G$, if $g \cdot x = h \cdot x$ then $g = h$. A bijection from G to X is then given by choosing any element $x \in X$ and defining a function $f : G \to X$ by $f(g) = g \cdot x$.

Problem 2.3 (Permutation Representations)**.** Let G be a group and let X be a G-set. For each $g \in G$, define the function $\lambda_g : X \to X$ by $\lambda_g(x) = g \cdot x$. Do the following:

(1) Show that λ_g is a bijection, i.e. $\lambda_g \in S_X$.

(2) Show that the function $\lambda : G \to S_X$ defined by $\lambda(g) = \lambda_g$ is a homomorphism.

(3) Show that the function λ defined in part (2) is injective if and only if the action of G on X is faithful.

(4) Deduce Cayley's Theorem from parts (2) and (3) applied to the left regular representation of G.

Solution 2.3.1 (Solution to Part (1))**.** We first show that λ_g is injective. Let $x, y \in X$ be arbitrary, and suppose that $\lambda_g(x) = \lambda_g(y)$. Then $g \cdot x = g \cdot y$. Hence

$$x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = y,$$

thus λ_g is injective.
Now I claim that λ_g is surjective. Let $x \in X$ be arbitrary. Then $g^{-1} \cdot x \in X$, and we have

$$\lambda_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x.$$

Thus λ_g is surjective, hence bijective.

Solution 2.3.2 (Solution to Part (2))**.** Let $g, h \in G$ be arbitrary. We want to show that $\lambda(gh) = \lambda(g)\lambda(h)$, i.e. $\lambda_{gh} = \lambda_g \circ \lambda_h$. Let $x \in X$ be arbitrary. We have

$$\lambda_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot \lambda_h(x) = \lambda_g(\lambda_h(x)) = (\lambda_g \circ \lambda_h)(x),$$

as desired.

Solution 2.3.3 (Solution to Part (3))**.** Suppose that the action of G on X is faithful, i.e. if $g \cdot x = x$ for all $x \in X$ then $g = e$. Suppose that $g \in \ker(\lambda)$. Then by definition, $\lambda_g = \lambda(g) = \mathrm{id}$, i.e. $\lambda_g(x) = x$ for all $x \in X$. But this says $g \cdot x = x$ for all $x \in X$. Since the action of G on X is faithful, we have $g = e$. Hence $ker(\lambda) = \{e\}$. Since λ is a homomorphism, this shows that λ is injective.

Suppose on the other hand that λ is injective, and suppose that $g \cdot x = x$ for all $x \in X$. Then $\lambda_g(x) = x$ for all $x \in X$, hence $\lambda(g) = \lambda_g = \mathrm{id} = \lambda_e = \lambda(e)$. Since λ is injective, we conclude $g = e$. Thus the action of G on X is faithful.

Solution 2.3.4. Let G act on itself by the left regular representation. As discussed in the solution to the previous problem, the action of G on itself is faithful, hence $\lambda : G \to S_G$ is an injective homomorphism. By the first isomorphism theorem, $G \cong \lambda(G) \leq S_G$, hence G is isomorphic to a subgroup of S_G. (Note: this is the *same* proof we originally gave of Cayley's theorem, but rephrased in a more sophisticated manner. Later on, if you learn a little category theory, you'll see even more general versions of this proof that cover some other algebraic structures as well).

Problem 2.4. How many different ways can the vertices of a hexagon be colored with the three colors red, green, and blue, up to *rotation* of the hexagon? What about if we allow all symmetries in D_6? Give an example of two colorings of the hexagon which are not equivalent in the first case, but are equivalent in the second case.

Solution 2.4.1. Number the vertices of the hexagon counter-clockwise from 1 through 6, and let r be the usual rotation in D_6, i.e. $r = (123456)$ as an element of S_6. The powers of r are all of the rotations of the hexagon; these are:

$$\mathrm{id}, (123456), (135)(246), (14)(25)(36), (153)(264), (165432).$$

By Burnside's theorem, plus our theorem about counting the number of fixed points, we have that the number of orbits of the action of the rotations on the set of colorings of the hexagon is

$$\frac{1}{6}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1) = 130.$$

Glad we didn't have to count those by hand!
Now, suppose we throw in all of the remaining elements of D_6. These are the 6 reflections:

$$(12)(36)(45), (14)(23)(56), (16)(25)(34), (26)(35), (13)(46), (15)(24).$$

So our expression for Burnside's theorem becomes:

$$\frac{1}{12}(3^6 + 3^1 + 3^2 + 3^3 + 3^2 + 3^1 + 3^3 + 3^3 + 3^3 + 3^4 + 3^4 + 3^4) = 92.$$

An example of two colorings that aren't equivalent via a rotation but are equivalent via a reflection:

$$(1,2,3,4,5,6) = (R,G,B,B,B,B) \text{ vs. } (G,R,B,B,B,B).$$

3. Rings

Problem 3.1 (The Group of Units)**.** Let R be a ring with unity. Show that the set of all elements in R which have a multiplicative inverse forms a group under multiplication, called the group of units of R. We denote this group by $R^\times$. What is $M_2^\times$? What is $\mathbb{Z}^\times$?

Solution 3.1.1. The operation in $R^\times$ is given by multiplication as elements of R. This is an associative operation since multiplication in R is assumed to be associative. We first check that $R^\times$ is closed under this operation. Let $a, b \in R^\times$ be arbitrary. Then a and b have multiplicative inverses a^{-1} and b^{-1} in R. We have:

$$(b^{-1}a^{-1})(ab) = b^{-1}1b = 1 = a1a^{-1} = (ab)(b^{-1}a^{-1}),$$

so ab has multiplicative inverse $b^{-1}a^{-1}$, hence in particular $ab \in R^\times$.
Since $1 \in R$ is its own multiplicative inverse, $1 \in R^\times$. Let $a \in R^\times$ be arbitrary. Then since $aa^{-1} = a^{-1}a = 1$, we have that a^{-1} has multiplicative inverse a, so $a^{-1} \in R^\times$ also, and clearly a^{-1} is the inverse of a for multiplication. Thus $R^\times$ is a group.

$M_2(\mathbb{R})^\times$ consists of those 2×2-real matrices which have a multiplicative inverse, i.e. this is $GL_2(\mathbb{R})$.

The only elements of $\mathbb{Z}$ which have a multiplicative inverse are 1 and -1, so $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

Problem 3.2. Do Judson, Ch. 14, Exercise 4.

Solution 3.2.1. (a) By the lattice isomorphism theorem, the ideals of $\mathbb{Z}/18\mathbb{Z}$ are in one-to-one correspondence with ideals of $\mathbb{Z}$ which contain $18\mathbb{Z}$. All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$ (or 0), and $18\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid 18$, i.e. $n = 1, 2, 3, 6, 9, 18$. The correspondence of the lattice isomorphism theorem takes $n\mathbb{Z}$ to $n\mathbb{Z}/18\mathbb{Z}$, so $\mathbb{Z}/18\mathbb{Z}$ has ideals:

$$(0) = 18\mathbb{Z}/18\mathbb{Z}, (9) = 9\mathbb{Z}/18\mathbb{Z}, (6) = 6\mathbb{Z}/18\mathbb{Z},$$

$$(3) = 3\mathbb{Z}/18\mathbb{Z}, (2) = 2\mathbb{Z}/18\mathbb{Z}, \text{ and } (1) = \mathbb{Z}/18\mathbb{Z}.$$

By the third isomorphism theorem,

$$\frac{\mathbb{Z}/18\mathbb{Z}}{n\mathbb{Z}/18\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z},$$

so $n\mathbb{Z}/18\mathbb{Z}$ is prime in $\mathbb{Z}/18\mathbb{Z}$ if and only if $\mathbb{Z}/n\mathbb{Z}$ is an integral domain, i.e. if and only if n is prime. Likewise $n\mathbb{Z}/18\mathbb{Z}$ is maximal in $\mathbb{Z}/18\mathbb{Z}$ if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field, which again occurs if and only if n is prime. So the prime

ideals and maximal ideals of $\mathbb{Z}/18\mathbb{Z}$ are the same, and they are (3) and (2).

(b) The same argument as in part (a) shows that the ideals of $\mathbb{Z}/25\mathbb{Z}$ are

$$(0) = 25\mathbb{Z}/25\mathbb{Z}, (5) = 5\mathbb{Z}/25\mathbb{Z}, \text{ and } (1) = \mathbb{Z}/25\mathbb{Z},$$

and (5) is both prime and maximal, while the others are neither.

(c) Let J be an ideal of $M_2(\mathbb{R})$. Suppose that $A \in J$ is a nonzero element, say

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

By multiplying A on the left or right by

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

we can swap the rows or columns of A and obtain a new element of J. By doing this, we can assume a is nonzero. Then J contains

$$\begin{pmatrix} 1/a & 0 \\ 0 & 1/a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Again, using the "swapping rows and columns" trick, we can also obtain the element

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

and so J contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

where I is the identity matrix. Hence J contains $B = BI$ for all $B \in M_2(\mathbb{R})$. Hence the only ideals of $M_2(\mathbb{R})$ are (0) and $M_2(\mathbb{R})$ itself. The whole ring $M_2(\mathbb{R})$ is not a prime or maximal ideal by definition. The ideal (0) is maximal, but not prime (this only can happen because $M_2(\mathbb{R})$ is not a commutative ring!). To see that (0) is not prime, note that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = 0.$$

(d) Suppose J is an ideal of $M_2(\mathbb{Z})$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an element of J. Then J contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix},$$

and likewise J contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix},$$

and similarly

$$\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} \in J.$$

I claim now that the set of entries of matrices in J is a subgroup of $\mathbb{Z}$. Clearly 0 is an entry of the zero matrix, which is in J. And if a and b are entries of some matrices in J, the above shows that

$$\begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in J,$$

so $a - b \in J$.

So, let $n\mathbb{Z} \subseteq \mathbb{Z}$ be the subgroup of $\mathbb{Z}$ consisting of all entries of matrices in J. Then I claim that J is the set $nM_2(\mathbb{Z})$ of all matrices of the form

$$\begin{pmatrix} na & nb \\ nc & nd \end{pmatrix}$$

with $a, b, c, d \in \mathbb{Z}$. Certainly J is a subset of $nM_2(\mathbb{Z})$ by the definition of n. On the other hand, if $na, nb, nc, nd \in n\mathbb{Z}$ are arbitrary, then these elements are entries of some four matrices in J, hence by the above argument (plus the swapping rows and columns trick), J contains the elements

$$\begin{pmatrix} na & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & nb \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ nc & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & nd \end{pmatrix}.$$

Thus J also contains the sum of these elements, and hence contains $nM_2(\mathbb{Z})$.

So, all ideals of $M_2(\mathbb{Z})$ are either 0 or of the form $nM_2(\mathbb{Z})$ for some $n \in \mathbb{N}$. It's easy to see that $nM_2(\mathbb{Z}) \subseteq mM_2(\mathbb{Z})$ if and only if $m|n$, so the maximal ideals of $M_2(\mathbb{Z})$ are exactly $pM_2(\mathbb{Z})$ for $p \in \mathbb{N}$ prime. On the other hand, $M_2(\mathbb{Z})$ has no prime ideals; the whole ring is by definition not a prime ideal. For any $n \geq 2$, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin nM_2(\mathbb{Z}).$$

But the product of these two elements is $0 \in nM_2(\mathbb{Z})$. So $nM_2(\mathbb{Z})$ is not prime. And (0) is not prime for the same reason.

(e) Since $\mathbb{Q}$ is a field, its only ideals are (0) and $(1) = \mathbb{Q}$. The ideal (0) is both prime and maximal since $\mathbb{Q}/(0) \cong \mathbb{Q}$ is a field.

TEST - 8

Ordered Integral Domains. The integer and rational numbers.

1. Show that if θ is a ring isomorphism from $\mathbb{Z}$ to itself then θ must be the identity.

   Solution: Since θ is a ring homomorphism then $\theta(xy) = \theta(x)\theta(y)$ and $\theta(x+y) = \theta(x) + \theta(y)$, for all $x, y \in \mathbb{Z}$. It was seen in class that $\theta(0) = 0$ and $\theta(1) = 1$. (If $\theta : R \longrightarrow$ is hom. of rings then θ(zero of the ring R) = zero of the ring S and θ(unity of R) = unity of S). Then if $n \in \mathbb{Z}$ we have that

   $$\theta(n) = \theta(n \cdot 1) = \theta(1 + 1 + ... + 1) = \theta(1) + \theta(1) + ...\theta(1) = n\theta(1) = n.$$

2. ★ Prove that $\mathbb{Z}[\sqrt{2}]$ is not well ordered.

   Solution: It is not well ordered because any well ordered integral domain must be isomorphic to the ring of integers and $\mathbb{Z}[\sqrt{2}]$ is not isomorphic to $\mathbb{Z}$:

   If $f : \mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{2}]$ was a ring isomorphism then $f(1) = 1$ and therefore $f(2) = f(1+1) = f(1) + f(1) = 2$. Furthermore if f is an isomorphism so it is $f^{-1} : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}$ and $f^{-1}(2) = 2$ (♣).

   Since f^{-1} is a ring isomorphism we have:

   $$f^{-1}(2) = f^{-1}(\sqrt{2}\sqrt{2}) = f^{-1}(\sqrt{2})f^{-1}(\sqrt{2}) = (f^{-1}(\sqrt{2}))^2$$

   Now using (♣)

   $$2 = f^{-1}(2) = (f^{-1}(\sqrt{2}))^2$$

   but $f^{-1}(\sqrt{2}) \in \mathbb{Z}$, say $f^{-1}(\sqrt{2}) = y$. And therefore $y^2 \in \mathbb{Z}$. Hence we have found an integer y such that $y^2 = 2$, and we know that it is impossible in $\mathbb{Z}$ to find such number.

3. Prove that if θ is a ring isomorphism between R and S and R is a field then S is a field.

   Solution: If R is a commutative ring the so it is S: If $s_1, s_2 \in S$ then there exist r_1 and r_2 in R such that $\theta(r_1) = s_1$ and $\theta(r_2) = s_2$ because θ is surjective. Using that θ is a ring hom. and that R is a commutative ring respectively we obtain:

   $$s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) = \theta(r_2 r_1) = \theta(r_2)\theta(r_1) = s_2 s_1.$$

   Therefore S is a commutative ring.

   The unity in S is $\theta(e_R)$. (It exists because θ is bijective.)

   Let us prove that if R is an integral domain then S is an integral domain:

Notice that if $s_1 s_2 = 0_S$ then there exist $r_1, r_2 \in R$ such that $s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) = 0_S$. But theta is a hom. which implies that $r_1 r_2 = 0_R$. Since R is an integral domain then either $r_1 = 0_R$ or $r_2 = 0_R$ and then $\theta(r_1) = s_1 = 0_S$ or $\theta(r_2) = s_2 = 0_S$. So S is an integral domain.

The existence of inverses follow since $s = \theta(r)$, for some $r \in R$, and R is a field there exist $r^{-1} \in R$ such that $rr^{-1} = e_R$ and since theta is hom. we get $\theta(rr^{-1}) = \theta(r)\theta(r^{-1}) = s\theta(r^{-1}) = e_S$ so the inverse for s is the unique $\theta(r^{-1})$.

The distributive laws are an exercise for the reader.

4. Use exercise 2 to prove that $\mathbb{Q}[\sqrt{2}]$ is not well ordered.

   Solution: If $\mathbb{Q}[\sqrt{2}]$ is well ordered then it would be isomorphic to $\mathbb{Z}$, which is impossible because $\mathbb{Q}[\sqrt{2}]$ is a field and $\mathbb{Z}$ is not.

5. ★ Verify that the field of quotients of $\mathbb{Z}[\sqrt{-2}]$ is isomorphic to $\mathbb{Q}[\sqrt{-2}]$.

   Solution: The isomorphism could be:

$$\theta([a+b\sqrt{-2}, c+d\sqrt{-2}]) = \frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{(c+d\sqrt{-2})(c-d\sqrt{-2})} = \frac{ac+bd}{c^2+2d^2} + \frac{bc-ad}{c^2+2d^2}\sqrt{-2}$$

It is homomorphism of rings:

$\theta([a+b\sqrt{-2}, c+d\sqrt{-2}] + [\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}])$

$= \theta((a+b\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2}) + (c+d\sqrt{-2})(\hat{a}+\hat{b}\sqrt{-2}), (c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})])$
using the definition of addition of classes in the quotient field

$= \dfrac{(a+b\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2}) + (c+d\sqrt{-2})(\hat{a}+\hat{b}\sqrt{-2})}{(c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})}$
using the definition of θ

$= \dfrac{(a+b\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})}{(c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})} + \dfrac{(c+d\sqrt{-2})(\hat{a}+\hat{b}\sqrt{-2})}{(c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})}$

$= \theta([a+b\sqrt{-2}, c+d\sqrt{-2}]) + \theta([\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}])$

$\theta([a+b\sqrt{-2}, c+d\sqrt{-2}][\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}])$

$= \theta((a+b\sqrt{-2})(\hat{a}+\hat{b}\sqrt{-2}), (c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})])$
using the definition of mulitplication of classes in the quotient field

$= \dfrac{(a+b\sqrt{-2})(\hat{a}+\hat{b}\sqrt{-2})}{(c+d\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2})}$
using the definition of θ

$= \dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} \dfrac{\hat{a}+\hat{b}\sqrt{-2}}{\hat{c}+\hat{d}\sqrt{-2}} = \theta([a+b\sqrt{-2}, c+d\sqrt{-2}])\theta([\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}])$

Now we need to prove that it is injective and well defined:

$$\theta([a+b\sqrt{-2}, c+d\sqrt{-2}]) = \theta([\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}])$$

if and only if

$$\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{\hat{a}+\hat{b}\sqrt{-2}}{\hat{c}+\hat{d}\sqrt{-2}}$$

and these two fractions are the same in the complex numbers if and only if

$$(a+b\sqrt{-2})(\hat{c}+\hat{d}\sqrt{-2}) = (\hat{a}+\hat{b}\sqrt{-2})(c+d\sqrt{-2})$$

which is equivalent to have

$$[a+b\sqrt{-2}, c+d\sqrt{-2}] = [\hat{a}+\hat{b}\sqrt{-2}, \hat{c}+\hat{d}\sqrt{-2}]$$

It is surjective:

Suppose $x+y\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}]$. Then there exits $a, b, c, d \in \mathbb{Z}$ such that $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Therefore:

$$x+y\sqrt{-2} = \frac{a}{b} + \frac{c}{d}\sqrt{-2} = \frac{ad+cb\sqrt{-2}}{bd} = \theta([ad+cb\sqrt{-2}, bd])$$

The exercises 6,7,8 are pretty similar to this one! (for example in 8 replace $\sqrt{-2}$ for $\sqrt{-1}$.)

6. Let $R = \{\frac{a}{2^k} : a, \in \mathbb{Z}, k \in \mathbb{N}\}$.
   - Prove that R is an integral domain.
   - Verify that the field of quotients of R is isomorphic to the field of the rational numbers.

TEST - 9

1. *Use Eisenstein's criterion to verify that the following polynomials are irreducible over* $\mathbb{Q}$*:—*

   (i) $x^2 - 2$*;*

   (ii) $x^3 + 9x + 3$*;*

   (iii) $x^5 + 26x + 52$.

   The requirements of Eisenstein' Criterion are satisfied with the prime number employed in that criterion equal to 2, 3 and 13 in cases (i), (ii) and (iii) respectively.

2. *The Fundamental Theorem of Algebra ensures that every non-constant polynomial with complex coefficients factors as a product of polynomials of degree one. Use this result to show that a non-constant polynomial with real coefficients is irreducible over the field* $\mathbb{R}$ *of real numbers if and only if it is either a polynomial of the form* $ax + b$ *with* $a \neq 0$ *or a quadratic polynomial of the form* $ax^2 + bx + c$ *with* $a \neq 0$ *and* $b^2 < 4ac$.

   Polynomials over the form $ax + b$ can only have factors of degrees zero and one and are thus irreducible. A quadratic polynomial of the form $ax^2 + bx + c$ with $a \neq 0$ and $b^2 < 4ac$ has non-real roots and therefore cannot be factored as a product of two polynomials of degree one. Such quadratic polynomials are thus irreducible over the field of real numbers.

   Let $f(x)$ be an polynomial with real coefficients that is irreducible over the field $\mathbb{R}$ of real numbers. It follows from the Fundamental Theorem of Algebra that the polynomial f has at least one root in the field of complex numbers. Let α be a root of f. If α is a real number then $x - \alpha$ is a factor of f in the polynomial ring $\mathbb{R}[x]$, and therefore $f(x) = a(x - \alpha)$, where a is the leading coefficient of f. If α is not a real number then its complex conjugate $\overline{\alpha}$ is also a root of f. But then $(x - \alpha)(x - \overline{\alpha})$ is a polynomial with real coefficients that divides the irreducible polynomial f in the polynomial ring $\mathbb{R}$. Indeed

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + |\alpha|^2 = x^2 + 2px + p^2 + q^2,$$

where the real numbers p and q are the real and imaginary parts respectively of the complex number α. It follows from the irreducibility of f that

$$f(x) = a(x-\alpha)(x-\overline{\alpha}) = ax^2 + bx + c,$$

where $b = 2pa$ and $c = (p^2+q^2)a$. Moreover

$$b^2 = 4p^2a^2 < 4(p^2+q^2)a^2 = 4ac.$$

It follows that a polynomial with real coefficients that is irreducible over the field of real numbers must either be of the form $ax+b$, where $a, b \in \mathbb{R}$ and $a \neq 0$, or else must be of the form ax^2+bx+c, where $a, b, c \in \mathbb{R}$, $a \neq 0$ and $b^2 < 4ac$.

3. *Let d be a rational number that is not the square of any rational number, let $\sqrt{d}$ be a complex number satisfying $(\sqrt{d})^2 = d$, and let L denote the set of all complex numbers that are of the form $a + b\sqrt{d}$ for some rational numbers a and b. Prove that L is a subfield of the field of complex numbers, and that $L:\mathbb{Q}$ is a finite field extension of degree 2.*

If $z_1, z_2 \in L$ then $z_1 + z_2 \in L$, $z_1 - z_2 \in L$ and $z_1 z_2 \in L$. Indeed if $z_1 = a_1 + b_1\sqrt{d}$ and $z_2 = a_2 + b_2\sqrt{d}$ then

$$\begin{aligned} z_1 + z_2 &= (a_1+a_2) + (b_1+b_2)\sqrt{d}, \\ z_1 - z_2 &= (a_1-a_2) + (b_1-b_2)\sqrt{d}, \\ z_1 z_2 &= (a_1a_2 + b_1b_2d) + (a_1b_2 + b_1a_2)\sqrt{d}. \end{aligned}$$

The set L is therefore a unital commutative ring. In order to show that L is a field, it remains to show that all non-zero elements of L are invertible. Let a and b be rational numbers that are not both zero. Then

$$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2d,$$

Moreover $b^2d \neq a^2$, because d is not the square of any rational number. It follows that the reciprocal of $a+b\sqrt{d}$ is in L for all $a+b\sqrt{d} \in L$, and

$$\frac{1}{a+b\sqrt{d}} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d}.$$

The elements 1 and $\sqrt{d}$ are linearly independent over the field of rational numbers, because $\sqrt{d}$ is not itself a rational number, and therefore the field L is a two-dimensional vector space over the field $\mathbb{Q}$ of rational numbers with basis $1, \sqrt{d}$.

4. *A complex number is said to be* algebraic *if it is a root of some non-zero polynomial f with rational coefficients. A complex number is thus algebraic if and only if it is algebraic over the field $\mathbb{Q}$ of rational numbers. Moreover a simple field extension $K(\alpha)\colon K$ is finite if and only if the adjoined element α is algebraic over the ground field K. Thus a complex number z is algebraic if and only if $\mathbb{Q}(z)\colon\mathbb{Q}$ is a finite field extension. Use the Tower Law to prove that the set of all algebraic numbers is a subfield of $\mathbb{C}$.*

   Let z and w be algebraic numbers. The algebraic number w is algebraic over the field $\mathbb{Q}$ and is therefore algebraic over the field $\mathbb{Q}(z)$. It follows that $\mathbb{Q}(z)(w)\colon\mathbb{Q}(z)$ is a finite field extension. Now $\mathbb{Q}(z)(w) = \mathbb{Q}(z, w)$, because both fields are the smallest subfields of the complex numbers that contain the rational numbers together with the complex numbers z and w. It follows from the Tower Law that $\mathbb{Q}(z, w)\colon\mathbb{Q}$ is a finite field extension. Now the elements $z + w$, $z - w$ and zw all belong to $\mathbb{Q}(z, w)$. It follows that the field extensions $\mathbb{Q}(z + w)\colon\mathbb{Q}$, $\mathbb{Q}(z - w)\colon\mathbb{Q}$ and $\mathbb{Q}(zw)\colon\mathbb{Q}$, are finite, and therefore the complex numbers $z+w$, $z-w$ and zw are algebraic numbers. Moreover if $w \neq 0$ then $zw^{-1} \in \mathbb{Q}(z, w)$ and therefore zw^{-1} is an algebraic number. Thus the set of all algebraic numbers is a subfield of the field $\mathbb{C}$ of complex numbers.

5. *Let L be a splitting field for a polynomial of degree n with coefficients in K. Prove that $[L\colon K] \leq n!$.*

   We prove the result by induction on n. If L is a splitting field for a polynomial $ax + b$ of degree 1 with coefficients a and b in K then the unique root of that polynomial is $-b/a$, which is in K, and therefore $L = K$ and $[L\colon K] = 1$. Thus the result holds for $n = 1$.

   Suppose that $[M\colon K] \leq m!$ whenever M is a splitting field for a polynomial g of degree m with coefficients in K. Let L be a splitting field over K for some polynomial f of degree $m + 1$ with coefficients in K. Then all roots of f are in L. Let α be one of the roots of f. Then $f(x) = (x - \alpha)g(x)$ for some polynomial g satisfying $\deg g = m$. The polynomial g splits over L, and therefore there is a unique subfield M of L that is a splitting field for M over K. The induction hypothesis ensures that $[M\colon K] \leq m!$. Now $L = M(\alpha)$. It follows from a standard result concerning simple algebraic extensions that $[L\colon M]$ is equal to the degree of the minimum polynomial of α over M. This minimum polynomial divides the polynomial f and therefore is at most $m+1$. It

follows from the Tower Law that

$$[L: K] = [L: M][M: K] \leq (m+1)[M: K] \leq (m+1)m! = (m+1)!,$$

as required.

6. (a) *Using Eisenstein's criterion, or otherwise, prove that* $\sqrt{3}$ *is not a rational number, and is not of the form* $b\sqrt{2}$ *for any rational number* b. *Hence or otherwise, show that there cannot exist rational numbers* a *and* b *such that* $\sqrt{3} = a + b\sqrt{2}$, *and thus prove that* $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

An immediate application of Eisenstein's criterion shows that the polynomial polynomial $x^2 - 3$ is irreducible over the field of rational numbers. This polynomial is thus the minimum polynomial of $\sqrt{3}$ over the field $\mathbb{Q}$ of rational numbers. An application of Eisenstein's criterion with prime number 3 shows that the polynomial $2x^2 - 3$ is also irreducible. It follows that $\sqrt{3}/\sqrt{2}$ is not a rational number.
If it were the case that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ then there would exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$. But then

$$3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{3}.$$

But $\sqrt{3} \notin \mathbb{Q}$. Therefore it would follow that $ab = 0$, and thus either $a = 0$ or $b = 0$. But $b = 0$ would imply that $\sqrt{3} \in \mathbb{Q}$, which is not the case, and $a = 0$ would imply that $\sqrt{3} = b\sqrt{2}$, which is not the case. Therefore there cannot exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$. It follows that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

(b) *Explain why* $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, *and, using the result of (a) and the Tower Law, or otherwise, prove that* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$.

Now $\mathbb{Q}(\sqrt{2}) \cup \{\sqrt{3}\} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and therefore

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Also $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\} \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$, and therefore

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}).$$

Therefore

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

It was shown in (a) that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. It follows that the polynomial $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$, and is therefore the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. It follows that $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, and thus $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. It then follows from the Tower Law that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4,$$

as required.

(c) *Show that* $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ *and* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$. *What is the degree of the minimum polynomial of* $\sqrt{2} + \sqrt{3}$ *over* $\mathbb{Q}$*?*

Clearly $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and therefore $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. To prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$, it suffices to show that $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Now $(\sqrt{2} + \sqrt{3})^n \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ for all positive integers n. Moreover

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^2 &= 2 + 3 + 2\sqrt{2}\sqrt{3} \\
&= 5 + 2\sqrt{6} \\
(\sqrt{2} + \sqrt{3})^3 &= (\sqrt{2} + \sqrt{3})(5 + 2\sqrt{6}) = 5\sqrt{2} + 5\sqrt{3} + 2\sqrt{12} + 2\sqrt{18} \\
&= 11\sqrt{2} + 9\sqrt{3}.
\end{aligned}$$

It follows that

$$\sqrt{2} = \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

But then

$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

It follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(d) *Show that* $\sqrt{2} + \sqrt{3}$ *is a root of the polynomial* $x^4 - 10x^2 + 1$, *and thus show that this polynomial is an irreducible polynomial whose splitting field over* $\mathbb{Q}$ *is* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Now

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^4 &= (\sqrt{2} + \sqrt{3})(11\sqrt{2} + 9\sqrt{3}) \\
&= 49 + 20\sqrt{6}
\end{aligned}$$

and therefore

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0.$$

Thus $(\sqrt{2}+\sqrt{3})^4$ is a root of the polynomial x^4-10x^2+1. But

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4,$$

and therefore the minimum polynomial of $\sqrt{2}+\sqrt{3}$ must be a monic polynomial of degree 4. This monic polynomial must also divide the polynomial x^4-10x^2+1. Therefore x^4-10x^2+1 is the minimum polynomial of $\sqrt{2}+\sqrt{3}$. Thus x^4-10x^2+1 is an irreducible polynomial whose splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(e) *Let φ_1 and φ_2 be $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Suppose that $\varphi_1(\sqrt{2}) = \varphi_2(\sqrt{2}) = \sqrt{2}$ and $\varphi_1(\sqrt{3}) = \varphi_2(\sqrt{3}) = \sqrt{3}$. Explain why $\varphi_1 = \varphi_2$.*

The set $\mathbb{Q}\cup\{\sqrt{2},\sqrt{3}\}$ is contained in the fixed field of $\varphi_2^{-1}\varphi_1$, and therefore the fixed field of $\varphi_2^{-1}\varphi_1$ must be the whole of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, and thus $\varphi_1 = \varphi_2$.

(f) *Prove that there exist $\mathbb{Q}$-automorphisms σ and τ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ satisfying*

$$\begin{array}{ll}\sigma(\sqrt{2}) = \sqrt{2}, & \sigma(\sqrt{3}) = -\sqrt{3};\\ \tau(\sqrt{2}) = -\sqrt{2}, & \tau(\sqrt{3}) = \sqrt{3};\end{array}.$$

The field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field for the polynomial x^2-3 over the field $\mathbb{Q}(\sqrt{2})$ Moreover the polynomial x^3-3 is irreducible over $\mathbb{Q}(\sqrt{2})$ and has roots $\sqrt{3}$ and $-\sqrt{3}$. It follows from the theory of isomorphisms of splitting fields that there exists an automorphism σ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ that fixes the subfield $\mathbb{Q}(\sqrt{2})$ and satisfies $\sigma(\sqrt{3}) = -\sqrt{3}$. Similarly there exists an automorphism τ of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ that fixes the subfield $\mathbb{Q}(\sqrt{3})$ and satisfies $\tau(\sqrt{2}) = -\sqrt{2}$.

(g) *Prove that the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, constitute a group of order 4 isomorphic to a direct product of two cyclic groups of order 2.*

Let ι denote the identity automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and let $G = \{\iota,\sigma,\tau,\sigma\tau\}$. Now

$$\begin{array}{ll}\iota(\sqrt{2}) = \sqrt{2}, & \iota(\sqrt{3}) = \sqrt{3};\\ \sigma(\sqrt{2}) = \sqrt{2}, & \sigma(\sqrt{3}) = -\sqrt{3};\\ \tau(\sqrt{2}) = -\sqrt{2}, & \tau(\sqrt{3}) = \sqrt{3};\\ \sigma\tau(\sqrt{2}) = -\sqrt{2}, & \sigma\tau(\sqrt{3}) = -\sqrt{3}.\end{array}$$

Moreover it follows from (e) that any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is determined by its action on $\sqrt{2}$ and $\sqrt{3}$. The possible images of $\sqrt{2}$ and $\pm\sqrt{2}$, and the possible images of $\sqrt{3}$ are $\pm\sqrt{3}$. It follows that the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ can have at most four $\mathbb{Q}$-automorhisms. Thus the group G is the group of $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Moreover $\sigma\tau = \tau\sigma$, since the composition of σ with τ in either order sends $\sqrt{2}$ to $-\sqrt{2}$ And sends $\sqrt{3}$ to $-\sqrt{3}$. It follows that the group G is isomorphic to the direct product of the two subgroups $\{\iota,\sigma\}$ and $\{\iota\tau\}$. These subgroups are of order 2.

7. *Let K be a field of characteristic p, where p is prime.*

(a) *Show that $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = g(x^p)$ for some $g \in K[x]$.*

Let

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n = \sum_{j=0}^{n} c_jx^k.$$

Then

$$(Df)(x) = \sum_{j=1}^{n} j.c_jx^{j-1}.$$

Now $j.c_j = (j.1_K)c_j$ for $j = 0, 1, \ldots, n$, where 1_K denotes the identity element of the field K. Also $j.1_K = 0_K$ if and only if j is divisible by the prime number p, because K is a field of characteristic p. Thus if $(Df) = 0$ then $(j.1_K)c_j = 0_K$ for all positive integers j satisfying $0 < j \leq n$, and therefore $c_j = 0_K$ for all positive integers j satisfying $0 < j \leq n$ that are not divisible by the prime number p. It follows that if $f \neq 0$ and $Df = 0$ then f is of degree mp for some non-negative integer p, and

$$f(x) = x_0 + c_px^p + c_{2p}x^{2p} + \cdots + c_{mp}x^{mp} = g(x^p),$$

where

$$g(x) = x_0 + c_px + c_{2p}x^2 + \cdots + c_{mp}x^m.$$

(b) *Let $h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $a_0, a_1, \ldots, a_n \in K$. Show that $(h(x))^p = g(x^p)$, where $g(x) = a_0^p + a_1^px + a_2^px^2 + \cdots + a_n^px^n$.*

Let $h_0(x)$ and $h_1(x)$ be polynomials with coefficients in the field K. Then

$$\Big(h_0(x)+h_1(x)\Big)^p = \sum_{j=0}^{p} \begin{pmatrix} p \\ j \end{pmatrix} \cdot h_0(x)^{p-j} h_1(x)^j = h_0(x)^p + h_1(x)^p.$$

Indeed the Commutative, Associative and Distributive Laws are satisfied in the polynomial ring $K[x]$, and therefore the appropriate form of the Binomial Theorem is applicable in this ring. But the binomial coefficient $\begin{pmatrix} p \\ j \end{pmatrix}$ is an integer divisible by p when $0 < j < p$, and therefore $\begin{pmatrix} p \\ j \end{pmatrix} \cdot f(x) = 0$ for all polynomials $f(x)$ with coefficients in the field K when $0 < j < p$.
It follows by induction on n that

$$\left(\sum_{k=0}^{n} h_k(x)\right)^p = \sum_{k=0}^{n} h_k(x)^p$$

for all $h_0, h_1, \ldots, h_n \in K[x]$. In particular, if $h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, then

$$h(x)^p = \left(\sum_{k=0}^{n} a_k x^k\right)^p = \sum_{k=0}^{n} a_k^p x^{kp} = g(x^p),$$

where $g(x) = a_0^p + a_1^p x + a_2^p x^2 + \cdots + a_n^p x^n$.

(c) *Now suppose that Frobenius monomorphism of K is an automorphism of K. Show that $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = (h(x))^p$ for some $h \in K[x]$. Hence show that $Df \neq 0$ for any irreducible polynomial f in $K[x]$.*

Suppose that $f \in K[x]$ satisfies $Df = 0$. Then $f(x) = g(x_p)$ for some $g \in K[x]$. Let $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$. Now, for each integer j between 0 and n there is some element a_j of K such that $a_j^p = c_j$, because the Frobenius monomorphism of K is an automorphism and is thus surjective. But then

$$g(x) = a_0^p + a_1^p x + a_2^p x^2 + \cdots + a_n^p x^n.$$

It follows from (b) that $f(x) = g(x^p) = h(x)^p$, where

$$h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

We conclude that if $f \in K[x]$ satisfies $Df = 0$ then $f(x) = h(x)^p$ for seom $h \in K[x]$.

We now verify the converse. A straightforward proof by induction on k shows that $D(h(x))^k = k.h(x)^{k-1}Dh(x)$ for all positive integers k. In particular $D(h(x))^p = p.h(x)^{p-1}Dh(x) = 0$. We conclude that if the Frobenius monomorphism of the field K is an automorphism, and if $f \in K[x]$ satisfies $Df = 0$ then $f(x) = h(x)^p$ for some $h \in K[x]$.

(d) *Use these results to show that every algebraic extension $L: K$ of a finite field K is separable.*

An irreducible polynomial $f \in K[x]$ is inseparable if and only if $Df = 0$. (see Corollary 6.8). But if K is a finite field, then every injective function from K to itself is surjective, and therefore every monomorphism from K to itself is an automorphism. In particular the Frobenius monomorphism of a finite field is an automorphism. It follows from (c) that a polynomial $f \in K[x]$ satisfies $Df = 0$ if and only if $f(x) = h(x)^p$ for some $h \in K[x]$. We conclude from this that no irreducible polynomial f with coefficients in K can satisfy $Df = 0$. Thus there are no inseparable polynomials with coefficients in a finite field K, and therefore every algebraic extension $L: K$ of a finite field K is separable.

8. *For each positive integer n, let ω_n be the primitive nth root of unity in $\mathbb{C}$ given by $\omega_n = \exp(2\pi i/n)$, where $i = \sqrt{-1}$. Explain why the field extensions $\mathbb{Q}(\omega_n): \mathbb{Q}$ and $\mathbb{Q}(\omega_n, i): \mathbb{Q}$ are normal field extensions for all positive integers n.*

The field $\mathbb{Q}(\omega_n)$ is a splitting field for the polynomial $x^n - 1$ over $\mathbb{Q}$, since the roots of this polynomial are powers of ω_n. Any splitting field extension is both finite and normal.

The field $\mathbb{Q}(\omega_n, i)$ is a splitting field for the polynomial $(x^n - 1)(x^2 + 1)$ over $\mathbb{Q}$. Any splitting field extension is both finite and normal.

9. (a) *Let p be a prime number. The* cyclotomic polynomial $\Phi_p(x)$ *is defined by*

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

Show that

$$x\Phi_p(x + 1) = (x + 1)^p - 1,$$

and hence show that

$$\Phi_p(x) = \sum_{k=0}^{p-1} \begin{pmatrix} p \\ k+1 \end{pmatrix} x^k,$$

where $\begin{pmatrix} p \\ k+1 \end{pmatrix}$ *is the binomial coefficient whose value is the number of ways of choosing* $k+1$ *objects from a collection of* p *objects.*

The cyclotomic polynomial $\Phi_p(x)$ satisfies the identity $(x-1)\Phi_p(x) = x^p - 1$. On substituting $x+1$ for x, we find that $x\Phi_p(x) = (x+1)^p - 1$. On expanding $(x+1)^p$ using the Binomial Theorem, we find that

$$x\Phi_p(x) = \sum_{k=1}^{p} \binom{p}{k} x^k.$$

On substituting $k+1$ for k in this formula, we find that

$$\Phi_p(x) = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k.$$

(b) *If* p *be a prime number, then the binomial coefficient* $\begin{pmatrix} p \\ k+1 \end{pmatrix}$ *is divisible by* p *for all integers* k *satisfying* $0 < k < p$. *By making use of this result or otherwise, show that the cyclotomic polynomial* $\Phi_p(x)$ *is irreducible over* $\mathbb{Q}$ *for all prime numbers* p.

The cyclotomic polynomial $\Phi_p(x)$ is a polynomial of degree $p-1$, and its leading coefficient $\begin{pmatrix} p \\ p \end{pmatrix}$ is equal to 1. The remaining coefficients of this polynomial are divisible by the prime number p. The constant coefficient is $\begin{pmatrix} p \\ 1 \end{pmatrix}$, and this coefficient has the value p. Therefore the constant coefficient of $\Phi_p(x)$ is not divisible by p^2. We have thus verified that the leading coefficient of $\Phi_p(x)$ is not divisible by the prime number p, the remaining coefficients are all divisible by p, and the constant coefficient is not divisible by p^2. The conditions of Eisenstein's criterion for irreducibility are therefore satisfied with respect to the prime number p. We conclude therefore that $\Phi_p(x)$ is an irreducible monic polynomial of degree $p-1$ over the field $\mathbb{Q}$ of rational numbers.

(c) *Let* p *be a prime number, and let* $\omega_p = \exp(2\pi i/p)$, *where* $i = \sqrt{-1}$. *Prove that the minimum polynomial of* ω_p *over* $\mathbb{Q}$ *is the* cyclotomic polynomial $\Phi_p(x)$, *where* $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$.

It was shown in (b) that, for each prime number p, the cyclotomic polynomial $\Phi_p(x)$ is an irreducible monic polynomial of degree $p-1$ over the field $\mathbb{Q}$ of rational numbers. It follows from this that it is the minimum polynomial of each of its roots. Those roots include ω_p.
Now the coefficient of x^k in $\Phi_p(x)$ is the binomial coefficient $\binom{p}{k+1}$. This coefficient is divisible by the prime number p for $0 \leq k < p-1$. Moreover the leading coefficient has the value 1, and constant coefficient has the value p. It follows from Eisenstein's Criterion, that the polynomial Φ_p is irreducible over $\mathbb{Q}$. Moreover it is a monic polynomial which has ω_p as a root. Therefore $\Phi_p(x)$ is the minimum polynomial of ω_p. It follows from a standard theorem concerning simple algebraic extensions that

$$[\mathbb{Q}(\omega_p):\mathbb{Q}] = \deg \Phi_p = p-1,$$

as required.

(d) *Explain why* $[\mathbb{Q}(\omega_p):\mathbb{Q}] = p-1$ *for all prime numbers* p, *where* $\omega_p = \exp(2\pi i/p)$.

The degree of the simple field extension $\mathbb{Q}(\omega_p):\mathbb{Q}$ is equal to the degree of the minimum polynomial of ω_p over the ground field $\mathbb{Q}$. But the minimum polynomial of ω_p over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_p(x)$, and this polynomial has degree $p-1$. The result follows.

10. *Throughout this question, let* $\omega = \omega_5 = \exp(2\pi i/5)$ *and* $\xi = \sqrt[5]{2}$. *Also let* $\Phi_5(x)$ *denote the cyclotomic polynomial*

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

The field $\mathbb{Q}(\omega)$ *is a splitting field for the polynomial* $\Phi_5(x)$ *over the field of rational numbers. Note that it was shown in Question 9 that the cyclotomic polynomial* $\Phi_5(x)$ *is irreducible over the field* $\mathbb{Q}$ *of rational numbers, and that therefore* $[\mathbb{Q}(\omega):\mathbb{Q}] = 4$.

(a) *Show that the field* $\mathbb{Q}(\xi,\omega)$ *is a splitting field for the polynomial* x^5-2 *over* $\mathbb{Q}$.

The roots of the polynomial x^5-2 in $\mathbb{C}$ are of the form $\xi\omega^r$ for $r = 0,1,2,3,4$. These roots all belong to the subfield $\mathbb{Q}(\xi,\omega)$ of $\mathbb{C}$. Let L be a subfield of $\mathbb{C}$ that contains all these roots. Then $\xi \in L$. Also L contains the ratio of the roots $\xi\omega$ and ξ, and therefore $\omega \in L$. Therefore $\mathbb{Q}(\xi,\omega) \in L$. Thus $\mathbb{Q}(\xi,\omega)$ is the smallest subfield of $\mathbb{C}$ that contains all rational numbers and also contains all the roots of the polynomial x^5-2. This field $\mathbb{Q}(\xi,\omega)$ is thus a splitting field for x^5-2 over $\mathbb{Q}$.

(b) *Show that* $[\mathbb{Q}(\xi,\omega):\mathbb{Q}] = 20$ *and* $[\mathbb{Q}(\xi,\omega):\mathbb{Q}(\omega)] = 5$. *Hence or otherwise, show that* $x^5 - 2$ *is the minimum polynomial of* $\xi\omega^s$ *over the field* $\mathbb{Q}(\omega)$ *for* $s = 0, 1, 2, 3, 4$.

The polynomial $x^5 - 2$ is irreducible, by Eisenstein's Criterion, with the prime number equal to 2, and therefore $[\mathbb{Q}(\xi):\mathbb{Q}] = 5$.

Now it follows from the Tower Law that $[\mathbb{Q}(\xi,\omega):\mathbb{Q}]$ is divisible by both $[\mathbb{Q}(\xi):\mathbb{Q}]$ and $[\mathbb{Q}(\omega):\mathbb{Q}]$, since $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\omega)$ are both subfields of $\mathbb{Q}(\xi,\omega)$. Thus $[\mathbb{Q}(\xi):\mathbb{Q}]$ is divisible by both 5 and 4, and is thus divisible by 20. But $\mathbb{Q}(\xi,\omega):\mathbb{Q}(\omega)$ is a simple algebraic extension, and the degree of this extension is equal to the degree of the minimum polynomial of ξ over $\mathbb{Q}(\omega)$. This minimum polynomial divides $x^5 - 2$. Therefore $[\mathbb{Q}(\xi,\omega):\mathbb{Q}(\omega)] \leq 5$. Now an immediate application of the Tower Law shows that

$$[\mathbb{Q}(\xi,\omega):\mathbb{Q}] = [\mathbb{Q}(\xi,\omega):\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}] \leq 20.$$

But we have already shown that this degree is divisible by 20. Therefore $[\mathbb{Q}(\xi,\omega):\mathbb{Q}] = 20$. Moreover $[\mathbb{Q}(\xi,\omega):\mathbb{Q}(\omega)] = 5$, and therefore the minimum polynomial of ξ over $\mathbb{Q}(\omega)$ is a monic polynomial of degree 5. We see from this that $x^5 - 2$ must be the minimum polynomial of ξ over $\mathbb{Q}(\omega)$. This polynomial is thus irreducible and is therefore the minimum polynomial of each of its roots over $\mathbb{Q}(\omega)$. These roots are of $\xi\omega^s$ over the field $\mathbb{Q}(\omega)$ for $s = 0, 1, 2, 3, 4$.

(c) *Prove that the Galois* $\Gamma(\mathbb{Q}(\xi,\omega):\mathbb{Q})$ *consists of the automorphisms* $\theta_{r,s}$ *for* $r = 1, 2, 3, 4$ *and* $s = 0, 1, 2, 3, 4$, *where* $\theta_{r,s}(\omega) = \omega^r$ *and* $\theta_{r,s}(\xi) = \omega^s\xi$.

The elements ξ and $\xi\omega$ of $\mathbb{Q}(\xi,\omega)$ have the same minimum polynomial over the field $\mathbb{Q}(\omega)$. A basic theorem in Galois Theory then ensures that there exists an automorphism σ of $\mathbb{Q}(\xi,\omega)$ such that $\sigma(\xi) = \xi\omega$ and $\sigma(z) = z$ for all $z \in \mathbb{Q}(\omega)$. Note that $\sigma(\omega) = \omega$.

Now it also follows from the Tower Law that

$$[\mathbb{Q}(\xi,\omega):\mathbb{Q}] = [\mathbb{Q}(\xi,\omega):\mathbb{Q}(\xi)][\mathbb{Q}(\xi):\mathbb{Q}],$$

where $[\mathbb{Q}(\xi,\omega):\mathbb{Q}] = 20$ and $[\mathbb{Q}(\xi):\mathbb{Q}] = 5$. It follows that

$$[\mathbb{Q}(\xi,\omega):\mathbb{Q}(\xi)] = 4.$$

Therefore the minimum polynomial Φ_5 of ω over $\mathbb{Q}$ is also the minimum polynomial of ω over $\mathbb{Q}(\xi)$. It follows that there exists an automorphism τ of $\mathbb{Q}(\xi,\omega)$ such that $\tau(\omega) = \omega^2$ and $\tau(z) = z$ for all

$z \in \mathbb{Q}(\xi)$. Note that $\tau(\xi) = \xi$. Moreover $\tau^2(\omega) = \tau(\tau(\omega)) = \omega^4$, and $\tau^3(\omega) = \tau(\tau^2(\omega)) = \omega^8 = \omega^3$. Let $\theta_{1,s} = \sigma^s$, $\theta_{2,s} = \sigma^s\tau$, $\theta_{3,s} = \sigma^s\tau^3$ and $\theta_{4,s} = \sigma^s\tau^2$. Then $\theta_{r,s}$ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\xi, \omega)$ for $r = 1, 2, 3, 4$ and $s = 0, 1, 2, 3, 4$. Also $\theta_{1,s}(\omega) = \sigma^s(\omega) = \omega$, $\theta_{2,s}(\omega) = \sigma^s(\tau(\omega))\sigma^s(\omega^2) = \omega^2$, $\theta_{3,s}(\omega) = \sigma^s(\tau^3(\omega))\sigma^s(\omega^3) = \omega^3$, and $\theta_{4,s}(\omega) = \sigma^s(\tau^2(\omega))\sigma^s(\omega^4) = \omega^4$ for $s = 0, 1, 2, 3, 4$. Also $\theta_{r,s}(\xi) = \sigma^s(\theta_{r,0}(\xi)) = \sigma^s(\xi) = \omega^s\xi$ for $r = 1, 2, 3, 4$ and $s = 0, 1, 2, 3, 4$. Thus we have 20 automorphisms $\theta_{r,s}$ that are distinct, and belong to the Galois Group $\Gamma(\mathbb{Q}(\xi, \omega) : \mathbb{Q})$. But this Galois Group is of order 20. Therefore any automorphism in this Galois group must be one of the automorphisms $\theta_{r,s}$.

11. *Let f be a monic polynomial of degree n with coefficients in a field K. Then*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f in some splitting field L for f over K. The discriminant *of the polynomial f is the quantity δ^2, where δ is the product $\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$ of the quantities $\alpha_j - \alpha_i$ taken over all pairs of integers i and j satisfying $1 \le i < j \le n$.*

Show that the quantity δ changes sign whenever α_i is interchanged with α_{i+1} for some i between 1 and $n - 1$. Hence show that $\theta(\delta) = \delta$ for all automorphisms θ in the Galois group $\Gamma(L : K)$ that induce even permutations of the roots of f, and $\theta(\delta) = -\delta$ for all automorphisms θ in $\Gamma(L : K)$ that induce odd permutations of the roots.

The quantity δ satisfies

$$(\alpha_{i+1} - \alpha_i)\rho\sigma\tau,$$

where

$$\rho = \prod_{\substack{1 \le j < k \le n \\ j \notin \{i, i+1\} \\ k \notin \{i, i+1\}}} (\alpha_k - \alpha_j)$$

$$\sigma = \prod_{1 \le k < i} ((\alpha_i - \alpha_k)(\alpha_{i+1} - \alpha_k))$$

$$\tau = \prod_{i+1 < k \le n} ((\alpha_k - \alpha_i)(\alpha_k - \alpha_{i+1}))$$

If α_i is interchanged with α_{i+1}, where $1 \leq i < n$, then the term $\alpha_{i+1} - \alpha_i$ changes sign, but the quantities ρ, σ and τ remain unchanged. Therefore the quantity δ changes sign when i is interchanged with $i+1$. Now any permutation of $\{1, 2, \ldots, n\}$ may be expressed as a composition of transpositions, and any transposition may be expressed as a composition of transpositions that swap adjacent integers in the list $1, 2, \ldots, n$. If a permutation is even, then it can be expressed as the composition of an even number of transpositions of this form; and if the permutation is odd, then it can be expressed as a composition of an odd number of transpositions of this form. Therefore δ is unchanged under an even permutation of the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, but changes sign under an odd permutation of these roots. Thus $\theta(\delta) = \delta$ for all $\theta \in \Gamma(L\colon K)$ that induce an even permutation of $\alpha_1, \alpha_2, \ldots, \alpha_n$, $\theta(\delta) = -\delta$ for all automorphisms θ in $\Gamma(L\colon K)$ that induce odd permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$.

It follows that $\theta(\delta^2) = (\theta(\delta))^2 = \delta^2$ for all $\theta\colon \Gamma(L\colon K)$. Therefore δ^2 belongs to the fixed field of $\Gamma(L\colon K)$.

12. *Let L be a splitting field for the polynomial f over the field K, where*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

Suppose that the field extension $L\colon K$ is separable, and is thus a Galois extension. Apply the Galois correspondence to show that the discriminant δ^2 of the polynomial f belongs to the field K containing the coefficients of f, and the field $K(\delta)$ is the fixed field of the subgroup of $\Gamma(L\colon K)$ consisting of those automorphisms in $\Gamma(L\colon K)$ that induce even permutations of the roots of f. Hence show that $\delta \in K$ if and only if all automorphisms in the Galois group $\Gamma(L\colon K)$ induce even permutations of the roots of f.

The splitting field extension $L\colon K$ is a Galois extension, because $L\colon K)$ is separable, and therefore the fixed field of $\Gamma(L\colon K)$ is the ground field K. We conclude that $\delta^2 \in K$.

Let H be the subgroup of $\Gamma(L\colon K)$ consisting of those permutations that induce even permutations of the roots of f, and let M be the fixed field of H. Then $\delta \in M$, and $K \subset M \subset L$. Now either $H = \Gamma(L\colon K)$, in which case $M = K$, or else H is a subgroup of $\Gamma(L\colon K)$ of index 2, in which case $[M\colon K] = 2$. (Indeed either all elements of $\Gamma(L\colon K)$ induce even permutations of the roots, or else half of them induce even permutations and the other half induce odd permutations.) If $H = \Gamma(L\colon K)$ then $M = K$ and $\delta \in K$, and thus $M = K(\delta)$. On the other

hand, if H is a proper subgroup of $\Gamma(L\colon K)$ then $\theta(\delta) = -\delta$ for some element θ of $\Gamma(L\colon K)$ that induces an odd permutation of the roots of f, and therefore $\delta \notin K$. But in that case $1 < [K(\delta)\colon K] \leq [M\colon K] = 2$, and therefore $K(\delta) = M$. Thus $K(\delta)$ is the fixed field of H. So we see that $\delta \in K$ if and only if $H = \Gamma(L\colon K)$, as required.

13. (a) *Show that the discriminant of the quadratic polynomial* $x^2 + bx + c$ *is* $b^2 - 4c$.

Let $x^2 + bx + c = (x - \alpha)(x - \beta)$. Then the discriminant is δ^2, where $\delta = (\beta - \alpha)$. Now $\alpha + \beta = -b$ and $\alpha\beta = c$. Therefore

$$\delta^2 = \alpha^2 + \beta^2 - 2\alpha\beta = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c.$$

(b) *Show that the discriminant of the cubic polynomial* $x^3 - px - q$ *is* $4p^2 - 27q^2$.

Let

$$x^3 - px - q = (x - \alpha)(x - \beta)(x - \gamma).$$

Then

$$\alpha + \beta + \gamma = 0, \quad p = -(\beta\gamma + \alpha\gamma + \alpha\beta), \quad q = \alpha\beta\gamma.$$

Moreover the discriminant is δ^2, where

$$\delta = (\beta - \alpha)(\gamma - \alpha)(\gamma - \beta).$$

Let us eliminate γ using the equation $\alpha + \beta + \gamma = 0$. We find that

$$\begin{aligned}
p &= \alpha^2 + \alpha\beta + \beta^2 \\
q &= -\alpha^2\beta - \alpha\beta^2 \\
\delta^2 &= (\beta - \alpha)^2(\alpha + 2\beta)^2(\beta + 2\alpha)^2 \\
&= (\alpha^2 - 2\alpha\beta + \beta^2)(2\alpha^2 + 2\beta^2 + 5\alpha\beta)^2 \\
&= (\alpha^2 - 2\alpha\beta + \beta^2)(4\alpha^4 + 20\alpha^3\beta + 33\alpha^2\beta^2 + 20\alpha\beta^3 + 4\beta^4) \\
&= 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 - 26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 \\
p^3 &= (\alpha^2 + \alpha\beta + \beta^2)(\alpha^4 + 2\alpha^3\beta + 3\alpha^2\beta^2 + 2\alpha\beta^3 + \beta^4) \\
&= \alpha^6 + 3\alpha^5\beta + 6\alpha^4\beta^2 + 7\alpha^3\beta^3 + 6\alpha^2\beta^4 + 3\alpha\beta^5 + \beta^6 \\
q^2 &= \alpha^2\beta^2(\alpha + \beta)^2 \\
&= \alpha^4\beta^2 + 2\alpha^3\beta^3 + \alpha^2\beta^4
\end{aligned}$$

Therefore

$$\delta^2 - 4p^3 = -27\alpha^4\beta^2 - 54\alpha^3\beta^3 - 27\alpha^2\beta^4 = -27q^2,$$

and thus $\delta^2 = 4p^2 - 27q^2$, as required.

14. *Let $f(x) = x^3 - px - q$ be a cubic polynomial with complex coefficients p and q without repeated roots, and let the complex numbers α, β and γ be the roots of f.*

(a) *Give formulae for the coefficients p and q of f in terms of the roots α, β and γ of f, and verify that $\alpha + \beta + \gamma = 0$ and*

$$\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q$$

The monic polynomial f has roots α, β and γ, and therefore

$$\begin{aligned} f(x) &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3 - (\alpha+\beta+\gamma)x^2 + (\beta\gamma+\alpha\gamma+\alpha\beta)x - \alpha\beta\gamma \end{aligned}$$

On comparing coefficients, we see that

$$\alpha + \beta + \gamma = 0, \quad p = -(\beta\gamma + \alpha\gamma + \alpha\beta), \quad q = \alpha\beta\gamma.$$

Then

$$\begin{aligned} 0 &= (\alpha+\beta+\gamma)^3 \\ &= \alpha^3 + 3\alpha^2(\beta+\gamma) + 3\alpha(\beta^2 + 2\beta\gamma + \gamma^2) \\ &\quad + \beta^3 + 3\beta^2\gamma + 3\beta\gamma^2 + \gamma^3 \\ &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3(\alpha^2(\beta+\gamma) + \beta^2(\alpha+\gamma) + \gamma^2(\alpha+\beta)) \\ &\quad + 6\alpha\beta\gamma \end{aligned}$$

But

$$\alpha^2(\beta+\gamma) + \beta^2(\alpha+\gamma) + \gamma^2(\alpha+\beta) = -(\alpha^3 + \beta^3 + \gamma^3),$$

because $\alpha + \beta + \gamma = 0$. It follows that

$$0 = -2(\alpha^3 + \beta^3 + \gamma^3) + 6\alpha\beta\gamma,$$

and therefore

$$\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma = 3q.$$

(b) *Let $\lambda = \alpha + \omega\beta + \omega^2\gamma$ and $\mu = \alpha + \omega^2\beta + \omega\gamma$, where ω is the complex cube root of unity given by $\omega = \frac{1}{2}(-1+\sqrt{3}i)$. Verify that $1+\omega+\omega^2 = 0$, and use this result to show that*

$$\alpha = \frac{1}{3}(\lambda + \mu), \qquad \beta = \frac{1}{3}(\omega^2\lambda + \omega\mu), \qquad \gamma = \frac{1}{3}(\omega\lambda + \omega^2\mu).$$

Calculating ω^2, we find that

$$\omega^2 = \tfrac{1}{4}\left(1 - 3 - 2\sqrt{3}i\right) = \tfrac{1}{2}\left(-1 - \sqrt{3}i\right).$$

It follows that $\omega + \omega^2 = -1$. Then

$$\begin{aligned} \lambda + \mu &= 2\alpha + (\omega + \omega^2)(\beta + \gamma) = (2 - \omega - \omega^2)\alpha = 3\alpha, \\ \omega^2\lambda + \omega\mu &= 2\beta + (\omega + \omega^2)(\alpha + \gamma) = (2 - \omega - \omega^2)\beta = 3\beta, \\ \omega\lambda + \omega^2\mu &= 2\gamma + (\omega + \omega^2)(\alpha + \beta) = (2 - \omega - \omega^2)\gamma = 3\gamma. \end{aligned}$$

(c) *Let K be the subfield $\mathbb{Q}(p, q)$ of $\mathbb{C}$ generated by the coefficients of the polynomial f, and let M be a splitting field for the polynomial f over $K(\omega)$. Show that the extension $M\colon K$ is normal, and is thus a Galois extension. Show that any automorphism in the Galois group $\Gamma(M\colon K)$ permutes the roots α, β and γ of f and either fixes ω or else sends ω to ω^2.*

The field M is a splitting field for the polynomial $f(x)(x^2 + x + 1)$ over the field K. It follows from a standard theorem that the extension $M\colon K$ is finite and normal. It is also separable, since the field K has characteristic zero. If $\sigma \in \Gamma(M\colon K)$ then $\sigma(p) = p$ and $\sigma(q) = q$. It follows that

$$\sigma(z^3 - pz - q) = \sigma(z)^3 - \sigma(p)\sigma(z) - \sigma(q) = \sigma(z)^3 - p\sigma(z) - q.$$

Thus σ sends any root of the polynomial $x^3 - px - q$ to another root of this polynomial. Therefore the elements of $\Gamma(M\colon K)$ permute the roots α, β and γ of the polynomial f. Similarly an element σ of $\Gamma(M\colon K)$ permutes the roots of the polynomial $x^2 + x + 1$. These roots are ω and ω^2. Therefore either $\sigma(\omega) = \omega$ or else $\sigma(\omega) = \omega^2$.

(d) *Let $\theta \in \Gamma(M\colon K)$ be a K-automorphism of M. Suppose that*

$$\theta(\alpha) = \beta, \quad \theta(\beta) = \gamma, \quad \theta(\gamma) = \alpha.$$

Show that if $\theta(\omega) = \omega$ then $\theta(\lambda) = \omega^2\lambda$ and $\theta(\mu) = \omega\mu$. Show also that if $\theta(\omega) = \omega^2$ then $\theta(\lambda) = \omega\mu$ and $\theta(\mu) = \omega^2\lambda$. Hence show that $\lambda\mu$ and $\lambda^3 + \mu^3$ are fixed by any automorphism in $\Gamma(M\colon K)$ that cyclically permutes α, β and γ. Show also that the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$ are also fixed by any automorphism in $\Gamma(M\colon K)$ that interchanges two of the roots of f whilst leaving the third root fixed. Hence prove that $\lambda\mu$ and $\lambda^3 + \mu^3$ belong to the field K generated by the coefficients of f and can therefore be expressed as rational functions of p and q.

Suppose that $\theta(\omega) = \omega$. Then

$$\begin{aligned}\theta(\lambda) &= \theta(\alpha) + \omega\theta(\beta) + \omega^2\theta(\gamma) = \beta + \omega\gamma + \omega^2\alpha = \omega^2\lambda.\\ \theta(\mu) &= \theta(\alpha) + \omega^2\theta(\beta) + \omega\theta(\gamma) = \beta + \omega^2\gamma + \omega\alpha = \omega\mu.\end{aligned}$$

(Here we have used the fact that $\omega^3 = 1$.) On the other hand, if $\theta(\omega) = \omega^2$ then $\theta(\omega^2) = \omega$, and therefore

$$\begin{aligned}\theta(\lambda) &= \theta(\alpha) + \omega^2\theta(\beta) + \omega\theta(\gamma) = \beta + \omega^2\gamma + \omega\alpha = \omega\mu.\\ \theta(\mu) &= \theta(\alpha) + \omega\theta(\beta) + \omega^2\theta(\gamma) = \beta + \omega^2\gamma + \omega^2\alpha = \omega^2\lambda.\end{aligned}$$

Thus if $\theta(\omega) = \omega$ then $\theta(\lambda^3) = \lambda^3$ and $\theta(\mu^3) = \mu^3$, and therefore $\theta(\lambda^3 + \mu^3) = \lambda^3 + \mu^3$. Similarly if if $\theta(\omega) = \omega^2$ then $\theta(\lambda^3) = \mu^3$ and $\theta(\mu^3) = \lambda^3$, and therefore $\theta(\lambda^3 + \mu^3) = \lambda^3 + \mu^3$. Also if $\theta(\omega) = \omega$ then $\theta(\lambda\mu) = (\omega^2\lambda)(\omega\mu) = \lambda\mu$. Similarly if $\theta(\omega) = \omega^2$ then $\theta(\lambda\mu) = (\omega\mu)(\omega^2\lambda) = \lambda\mu$. Now any element of the Galois group $\Gamma(M\colon K)$ that cyclicly permutes the roots α, β and γ of $f(x)$ is in the cyclic subgroup generated by the automorphism θ. We conclude that any element of the Galois group $\Gamma(M\colon K)$ that cyclicly permutes the roots α, β and γ of $f(x)$ must fix the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$.

Now suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_α which fixes α and interchanges β and γ. If $\tau_\alpha(\omega) = \omega$ then $\tau_\alpha(\lambda) = \mu$ and $\tau_\alpha(\mu) = \lambda$, and therefore τ_α fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\alpha(\omega) = \omega^2$, then $\tau_\alpha(\lambda) = \lambda$ and $\tau_\alpha(\mu) = \mu$, and therefore τ_α fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

Next suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_β which fixes β and interchanges α and γ. If $\tau_\beta(\omega) = \omega$ then $\tau_\beta(\lambda) = \omega^2\mu$ and $\tau_\beta(\mu) = \omega\lambda$, and therefore τ_β fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\beta(\omega) = \omega^2$, then $\tau_\beta(\lambda) = \omega\lambda$ and $\tau_\beta(\mu) = \omega^2\mu$, and therefore τ_β fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

Next suppose that $\Gamma(M\colon K)$ contains a K-automorphism τ_γ which fixes γ and interchanges α and β. If $\tau_\gamma(\omega) = \omega$ then $\tau_\gamma(\lambda) = \omega\mu$ and $\tau_\gamma(\mu) = \omega^2\lambda$, and therefore τ_γ fixes $\lambda\mu$ and $\lambda^3 + \mu^3$. Similarly if $\tau_\gamma(\omega) = \omega^2$, then $\tau_\gamma(\lambda) = \omega^2\lambda$ and $\tau_\gamma(\mu) = \omega\mu$, and therefore τ_γ fixes $\lambda\mu$ and $\lambda^3 + \mu^3$.

We have thus shown that every element of the Galois group $\Gamma(M\colon K)$ must fix the quantities $\lambda\mu$ and $\lambda^3 + \mu^3$. These quantities must therefore belong to the fixed field of the Galois group. This fixed field is the field K. Therefore $\lambda\mu \in K$ and $\lambda^3 + \mu^3 \in K$. These quantities must therefore be expressible in terms of the formulae constructed out of rational numbers and the quantities p and q using only the operations of addition, subtraction, multiplication and division.

(e) *Show by direct calculation that* $\lambda\mu = 3p$ *and* $\lambda^3 + \mu^3 = 27q$. *Hence show that* λ^3 *and* μ^3 *are roots of the quadratic polynomial* $x^2 - 27qx + 27p^3$. *Use this result to verify that the roots of the cubic polynomial* $x^3 - px - q$ *are of the form*

$$\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}$$

where the two cube roots must be chosen so as to ensure that their product is equal to $\frac{1}{3}p$.

By direct calculation, using the identity $\omega^3 = 1$, we see that

$$\begin{aligned}\lambda\mu &= \alpha^2 + \beta^2 + \gamma^2 + (\omega + \omega^2)(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= (\alpha + \beta + \gamma)^2 + (\omega + \omega^2 - 2)(\alpha\beta + \alpha\gamma + \beta\gamma).\end{aligned}$$

But $\alpha + \beta + \gamma = 0$ and $\omega^2 + \omega + 1 = 0$. Therefore

$$\lambda\mu = -3(\alpha\beta + \alpha\gamma + \beta\gamma) = 3p.$$

Also

$$\begin{aligned}\lambda^3 &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3\alpha^2(\omega\beta + \omega^2\gamma) + 3\beta^2(\omega^2\alpha + \omega\gamma) + 3\gamma^2(\omega\alpha + \omega^2\beta) \\ &\quad + 6\alpha\beta\gamma, \\ \mu^3 &= \alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3\alpha^2(\omega^2\beta + \omega\gamma) + 3\beta^2(\omega\alpha + \omega^2\gamma) + 3\gamma^2(\omega^2\alpha + \omega\beta) \\ &\quad + 6\alpha\beta\gamma.\end{aligned}$$

It follows that

$$\begin{aligned}\lambda^3 + \mu^2 &= 2\alpha^3 + \beta^3 + \gamma^3 \\ &\quad + 3(\omega + \omega^2)(\alpha^2(\beta + \gamma) + \beta^2(\alpha + \gamma) + \gamma^2(\alpha + \beta)) \\ &\quad + 12\alpha\beta\gamma,\end{aligned}$$

It follows that

$$\begin{aligned}\lambda^3 + \mu^2 &= (2 - 3\omega - 3\omega^2)(\alpha^3 + \beta^3 + \gamma^3) + 12\alpha\beta\gamma \\ &= 5(\alpha^3 + \beta^3 + \gamma^3) + 12\alpha\beta\gamma.\end{aligned}$$

Also $\alpha^3+\beta^3+\gamma^3 = 3\alpha\beta\gamma = 3q$. Therefore $\lambda^3+\mu^3 = 27q$. Now λ^3 and μ^3 are the roots of the quadratic polynomial $g(x)$, where

$$g(x) = (x-\lambda^3)(x-\mu^3) = x^2 - 27qx + 27p^3.$$

Now the roots of this quadratic polynomial are $r_\pm$, where

$$r_\pm = 27\left(\frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}\right).$$

One of these roots is λ^3, and the other is μ^3. The formula for the roots of the cubic polynomial are then given in terms of λ and μ by the formulae

$$\alpha = \frac{1}{3}(\lambda+\mu), \qquad \beta = \frac{1}{3}(\omega^2\lambda+\omega\mu), \qquad \gamma = \frac{1}{3}(\omega\lambda+\omega^2\mu).$$

TEST - 10

Presentation Problems:

1. Let R be a commutative ring and $\{a_1,\ldots,a_n\} \subseteq R$. Show that the set

$$I = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\} = \langle a_1, a_2, \ldots, a_n\rangle$$

is an ideal in R.

Proof: Recall that an ideal $I \subseteq R$ is an ideal if $(I,+)$ is an additive subgroup of $(R,+)$ such that I satisfies the absorption properties, i.e. for all $r \in R$ we have $rI \subseteq I$ and $Ir \subseteq I$. We first show that $(I,+)$ is an additive subgroup.
[closure:] Let $r_1a_1 + \cdots + r_na_n, s_1a_1 + \cdots + s_na_n \in I$. Then by associativity and distribution laws in R we have

$$(r_1a_1 + \cdots + r_na_n) + (s_1a_1 + \cdots + s_na_n) = (r_1+s_1)a_1 + \cdots + (r_n+s_n)a_n.$$

Clearly we have that $r_i + s_i \in R$ for all $1 \le i \le n$ and so I is closed under addition.
[absorption:] Let $r \in R$. Note that since R is commutative it is sufficient to just check $rI \subseteq I$. Every element of rI is of the form $r(r_1a_1 + \cdots + r_na_n)$. Again by associativity and distribution laws we have that

$$r(r_1a_1 + \cdots + r_na_n) = (rr_1)a_1 + \cdots + (rr_n)a_n.$$

We clearly see that $rr_i \in R$ for all $1 \le i \le n$ and so we have that $r(r_1a_1 + \cdots + r_na_n) \in I$. Since our choice of $r_1a_1 + \cdots + r_na_n$ was arbitrary, we have that the absorption property is satisfied.

2. Let $\varphi : F \to R$ be a ring homomorphism where F is a field and R is a ring. Show that either φ is one-to-one or is the zero homomorphism.

Proof: Recall that since φ is a ring homomorphism, $\ker\varphi$ is an ideal in the domain F. Since F is a field, the only possibilities for $\ker\varphi$ are the 0-ideal or all of F. If $\ker\varphi = \langle 0\rangle = 0$ then we know that φ is one to one. If $\ker\varphi = F$ then we know that $\varphi(a) = 0$ for all $a \in F$ and so φ is the zero homomorphism.

Problems to be turned in:

1. Let I and J be ideals in a ring R.

Note that since I, J are ideals in R we have that both $(I, +)$ and $(J, +)$ are additive subgroups of $(R, +)$ and that for all $r \in R$ we have that $rI, Ir \subseteq I$ and $rJ, Jr \subseteq J$. So in each part of this problem all we need to do is show that the set in question is a subgroup of R under addition and that the absorption properties are satisfied. The problem does not tell us that R is commutative so we will have to check both absorption properties in each case.

(a) Show that $I \cap J$ is an ideal in R.

Proof: Since we already know that I and J are additive subgroups of R, we know from group theory that their intersection is also a sugroup of R under addition. All that is left is to show absorption. Let $r \in R$ and $k \in I \cap J$. Since I and J satisfy the absorption property we have that $rk, kr \in I$ and $rk, kr \in J$ and so we must have that $rk, kr \in I \cap J$ and so $r(I \cap J), (I \cap J)r \subseteq I \cap J$.

(b) Show that $I + J := \{i + j \mid i \in I, j \in J\}$ is an ideal and that $I, J \subseteq I + J$ in R. This is called the **sum** of I and J.

Proof: We first show that $I + J$ is an additive subgroup and so we just need to show closure under addition and that additive inverses exist. Let $i_1 + j_1, i_2 + j_2 \in I + J$. Then by associativity and commutativity of addition we have

$$(i_1 + j_1) + (i_2 + j_2) = \underbrace{(i_1 + i_2)}_{\in I} + \underbrace{(j_1 + j_2)}_{\in J}.$$

Since I and J themselves are additive subgroups, they are closed under addition and so $i_1 + i_2 \in I$ and $j_1 + j_2 \in J$ and so $(i_1 + j_1) + (i_2 + j_2) \in I + J$. Also since I and J are subgroups, we have that for any $i \in I$ and $j \in J$ that $-i \in I$ and $-j \in J$ and so $(-i) + (-j) \in I + J$ and furthermore $(i + j) + ((-i) + (-j)) = 0$. So the sum of two ideals is indeed an additive subgroup.

Now we need to check the absorption properties. These will follow easily from the distributive laws. Let $r \in R$ and $i + j \in I + J$. Then $r(i + j) = ri + rj$ and we know that $ri \in I$ and $rj \in J$ since I and J satisfy the absorption properties. Therefore $r(i + j) \in I + J$. The exact same argument shows that $(i + j)r \in I + J$.

(c) Show that $IJ := \{\sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J, n \in \mathbb{Z}^+\}$ is an ideal and that $IJ \subseteq I \cap J$ in R. This is called the **product** of I and J

Proof: First note that the number of terms in the sums that define the set IJ is not fixed and can vary. Now we first show IJ is a subgroup of R under addition. To show closure let $\sum_{k=1}^{n} i_{1,k} j_{1,k}, \sum_{l=1}^{m} i_{2,l} j_{2,l} \in IJ$. Note that to have sufficient generality these sums have a different number of terms and the double index indicates that the terms themselves are different. Clearly we have that $\sum_{k=1}^{n} i_{1,k} j_{1,k} + \sum_{l=1}^{m} i_{2,l} j_{2,l}$ is just a sum of $n + m$ terms each of which is a a product of an element of I and an element of J and so their sum is in IJ. To show additive inverses exist,

let $\sum_{k=1}^{n} i_k j_k \in IJ$. Again, since I is an additive subgroup of R itself, we know that for all $1 \leq k \leq n$, $-i_k \in I$ and so $\sum_{k=1}^{n} (-i_k) j_k = -\sum_{k=1}^{n} i_k j_k \in IJ$ and $\sum_{k=1}^{n} i_k j_k + (-\sum_{k=1}^{n} i_k j_k) = 0$ as desired.
We now move on to showing the absorption properties. Let $r \in R$ and $\sum_{k=1}^{n} i_k j_k \in IJ$. Then by distributive and associative properties of R we have that

$$r \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n} r i_k j_k = \sum_{k=1}^{n} \underbrace{(r i_k)}_{\in I} j_k \tag{1}$$

$$\left(\sum_{k=1}^{n} i_k j_k \right) r = \sum_{k=1}^{n} i_k j_k r = \sum_{k=1}^{n} i_k \underbrace{(j_k r)}_{\in J}. \tag{2}$$

Since I and J are ideals and satisfy absorption properties we have that $r i_k \in I$ and $j_k r \in J$ for all $1 \leq k \leq n$ and so both $r \sum_{k=1}^{n} i_k j_k$ and $(\sum_{k=1}^{n} i_k j_k) r$ are in IJ which gives us absorption.

(d) Show that $I : J := \{r \in R \mid rj \in I \ \forall \ j \in J\}$ is an ideal in R.

Proof: Let's go ahead and show $I : J$ is an additive subgroup. Suppose $r_1, r_2 \in I : J$ and so for all $j \in J$ we have that $r_1 j, r_2 j \in I$. We want to show that $r_1 + r_2$ also satisfies this property. Let $j \in J$ and consider $(r_1 + r_2)j = r_1 j + r_2 j$. Since both $r_1 j$ and $r_2 j$ are in I, so must be their sum since I is closed under addition. Therefore we must have that $(r_1 + r_2)j \in I$ and so $r_1 + r_2 \in I : J$. Now we want to show $I : J$ contains additive inverses. Let $r \in I : J$. Then $rj \in I$ for all $j \in J$. Again, since I is an additive subgroup we must also have $-(rj) \in I$ but $-(rj) = (-r)j$ and so we must have $-r \in I : J$. Therefore we have that $I : J$ is an additive subgroup of R.
We now proceed to show absorption. Let $s \in R$ and $r \in I : J$. To show $sr, rs \in I : J$ we need to show for all $j \in J$ that $(sr)j, (rs)j \in I$. Note that since $r \in I : J$ we have $rj \in I$ and since I is an ideal we have that $(sr)j = s(rj) \in I$. Similarly, since J is an ideal we know that $sj \in J$ and since $r \in I : J$ we have that $(rs)j = r(sj) \in I$. And the result follows.