First Year Algebra Review

Jay Pantone
University of Florida

Last Edited: April 21, 2012

Contents

Preface

This packet consists practice problems, important theorems, and other reference material, that should help students prepare for their Master's exam in Algebra. The exercises in the First Year Pool are from an unofficial list distributed by the algebra committee. Questions on the actual exam may come from this list, or may be completely original. The proofs of these exercises are due to either myself, other graduate students or professors, or from algebra texts (such as Dummit & Foote). The sections on Important Theorems and Popular Examples & Counterexamples are mostly due to Dummit & Foote. There is a short section [which is mostly incomplete] with solutions to some past exams.

There are likely many typos and a few errors. If you find any please send them to me at jay.pantone@gmail.com. Additionally, if you write up (handwritten or typed) solutions to other past exams or other problems, you may send them to me and I will add them. Suggestions and criticism are also welcome.

Chapter 1

First Year Pool

This pool of questions comes from a list of 113 questions posted on the web pages of some members of the Algebra committee. This list was compiled by a graduate student many years ago, and is in no way official. Some questions fall into more than one category and so in ambiguous cases I have kept the original ordering of the questions.

1.1 List of Exercises

1 State and prove Cayley's Theorem about finite groups.

2 (a) Compute the order of the general linear group $GL_n(\mathbb{Z}_p)$, with p a prime number.

(b) Calculate the order of the subgroup $SL_n(\mathbb{Z}_p)$ of matrices which have determinant 1.

3 (a) Prove that two elements of the symmetric group S_n are conjugate if and only if their cycle types are the same.

(b) Is this true for the alternating groups? Justify your answer.

4 Prove that if $|G| = 12$ and G has 4 Sylow 3-subgroups, then $G \cong A_4$.

5 Let p and q be prime numbers, and suppose that $p < q$. If G is a group of order pq and p does not divide $q - 1$, show that G must be cyclic.

6 Recall that a group G is called a *p-group* (p a prime number) if for each $g \in G$, $g^{p^i} = 1$, for some positive integer i.

(a) Prove that if G is a finite p-group, then its center is not trivial.

(b) Use this fact to prove that every finite p-group is nilpotent.

7 Suppose that $\varphi : G \to H$ and $\theta : G \to K$ are homomorphisms between groups. Assume that φ is surjective. Show that if $\mathrm{Ker}(\varphi)$ is contained in $\mathrm{Ker}(\theta)$ then there is a unique homomorphism $\theta^* : H \to K$ such that $\theta^* \circ \varphi = \theta$.

8 Prove that if G is a finite group then any subgroup of index 2 is normal.

9 Prove that any subgroup of a cyclic group is cyclic.

10 Find all the automorphisms of order 3 in Z_{91}. (Hint: How can Z_3 act non-trivially on Z_{91}?) Does Z_{91} have any automorphisms of order 5? Explain.

11 Suppose that G is a nonabelian group of order 21. Prove:

(a) $Z(G) = \{e\}$;

(b) G has an automorphism which is not inner.

12 Let $GL_2(\mathbb{Z}_3)$ act on the four one-dimensional subspaces of $\mathbb{Z}_3^2$ by $g(\text{Span}\{v\}) = \text{Span}\{gv\}$, where $g \in GL_2(\mathbb{Z}_3)$ and $v \in \mathbb{Z}_3^2$. Prove that this action induces a surjective homomorphism of $GL_2(\mathbb{Z}_3)$ onto S_4 whose kernel is the subgroup of all scalar matrices.

13 Let p be a prime number and n be a positive integer. Prove that the general linear group $GL_n(\mathbb{Z}_p)$ is isomorphic to the automorphism group of $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (n times).

14 Suppose that $\varphi : G \to H$ is a surjective homomorphism of groups. Prove the following about the assignment $\varphi^* : N \mapsto \varphi^{-1}(N)$. Assume that it maps subgroups to subgroups.

(a) φ^* is a bijection between the lattice of subgroups of H and the set of subgroups of G that contain $\text{Ker}(\varphi)$.

(b) $N_1 \subseteq N_2$ if and only if $\varphi^*(N_1) \subseteq \varphi^*(N_2)$.

(c) $\varphi^*(N)$ is normal in G if and only if N is normal in H.

15 Let G be a finite group acting on the set S. Suppose that H is a normal subgroup of G so that for any $s_1, s_2 \in S$, there is a unique $h \in H$ so that $hs_1 = s_2$. For each $s \in S$, let $G_s = \{g \in G : gs = s\}$. Prove:

(a) $G = G_s H$, and $G_s \cap H = \{e\}$;

(b) if H is contained in the center of G, then G_s is normal and G is (isomorphic to) a direct product of G_S and H.

16 Suppose that G is a group and H is a proper subgroup of index k. Show that

(a) $g * (xH) = gxH$ defines a group action of G on the set $\Omega = (G/H)_\ell$ of left cosets of H;

(b) the kernel of the induced homomorphism into the permutation group on Ω is the intersection of all conjugates of H.

(c) Now suppose that G is simple and that $k > 1$ is the index of H. Then show that G is isomorphic to a subgroup of S_k.

17 Prove that a group of order 30 must have a normal subgroup of order 15.

18 Classify the groups of order 70.

19 Show that if G is a subgroup of S_n (n a natural number) containing an odd permutation, then half the elements of G are odd and half are even.

20 Use #19 to prove that if G is a group of order $2m$, with m odd, then G cannot be simple, and, indeed, contains a subgroup of index 2.

21 Classify the groups of order $4p$, where $p \geq 5$ is prime.

22 Let p be an odd prime number.

(a) Prove that in $GL_2(\mathbb{Z}_p)$ every element A of order 2, $A \neq -I$, is conjugate to the diagonal matrix U, for which $U_{1,1} = -1$ and $U_{2,2} = 1$.

(b) Now classify the groups of order $2p^2$, for which the Sylow p-subgroups are *not* cyclic.

23 (a) Prove that there are exactly four homomorphisms from Z_2 into $\mathrm{Aut}(Z_8)$.

(b) Show that these yield four pairwise nonisomorphic semidirect products.

24 Prove that S_4 contains no nonabelian simple groups.

25 Use the result of **Exercise 24** to prove that if G is a nonabelian simple group, then every proper subgroup of G has index at least 5.

26 Prove that D_{2n} is nilpotent if and only if n is a power of 2. (Hint: Use the ascending central chain; recall that if there is an even number of vertices n, then $Z(D_{2n}) \neq \{e\}$.

27 Let G be the group of all 3 by 3 upper triangular matrices, with entries in $\mathbb{Z}$, and diagonal entries equal to 1. Prove that the commutator of G is its center.

28 Let P be a Sylow p-subgroup of H and $H \leq K$. If P is normal in H and H is normal in K, prove that P is normal in K. Deduce that if $P \in \mathrm{Syl}_p(G)$ then $N_G(P)$ is self-normalizing, i.e., $N_G(N_G(P)) = N_G(P)$.

29 Prove that if G is a finite group, and each Sylow p-subgroup is normal in G, then G is a direct product of its Sylow subgroups.

30 Classify the abelian groups of order $2^5 \cdot 5^2 \cdot 17^3$.

31 Prove that $(\mathbb{Q}, +)$, the additive group of rational numbers is not cyclic.

32 Prove that $\mathrm{Aut}(Z_k)$ is isomorphic to the group $U(k)$ of integers i, with $1 \leq i < k$, which are relatively prime to K, under multiplication modulo k.

33 Give examples of each of the following, with a brief explanation in each case:

(a) A solvable group with trivial center.

(b) An abelian p-group which is isomorphic to one of its proper subgroups and also one of its proper homomorphic images.

(c) An abelian group having no maximal subgroups.

(d) A direct product of nilpotent groups which is not nilpotent.

(e) A semidirect product of abelian groups which is not nilpotent.

(f) A finite nonabelian group in which every proper subgroup is cyclic.

34 Each three-cycle in S_n has $\frac{1}{3}n(n-1)(n-2)$ conjugates. Prove this and conclude from it that A_4 is the only subgroup of S_4 of order 12.

35 Prove that A_5 is a simple group.

36 For $n \geq 5$, prove that A_n is the only proper, nontrivial normal subgroup of S_n.

37 Let G be a finite group. Call $x \in G$ a *non-generator* if for each subset $Y \subseteq G$, if $G = \langle Y \cup \{x\} \rangle$ then $G = \langle Y \rangle$. Prove:

(a) The subset $\Phi(G)$ of all non-generators of G form a subgroup of G.

(b) $\Phi(G)$ is the intersection of all maximal subgroups of G.

(c) Conclude from (b) that $\Phi(G)$ is normal.

(d) What is the Frattini subgroup $\Phi(S_n)$? Explain. (Consider the stabilizers of a single letter.)

38 State and prove the Orbit-Stabilizer Theorem.

39 Show that if G is a simple abelian group then it is cyclic of prime order.

40 For the additive group of rational numbers $(\mathbb{Q}, +)$, show that the intersection of any two nontrivial subgroups is nontrivial.

41 Show that the group $(\mathbb{Q}, +)$ of additive rational numbers has no maximal subgroups.

42 The *commutator subgroup* G' of a group G is defined as the subgroup generated by the set

$$\{x^{-1}y^{-1}xy \mid x, y \in G\}.$$

Prove that:

(a) Show that G' is a normal subgroup of G.

(b) Show that G/G' is abelian.

(c) Show that if $\varphi : G \to H$ is a homomorphism into the abelian group H, then there exists a unique homomorphism $\widehat{\varphi} : G/G' \to H$ such that $\widehat{\varphi}(xG') = \varphi(x)$, for each $x \in G$.

43 Suppose that G is a group and H is a normal subgroup. Prove that $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

44 Let G be a group of 385 elements. Prove that the Sylow 11-subgroups are normal, and that any Sylow 7-subgroup lies in the center.

45 Describe all groups of 44 elements, up to isomorphism.

46 Suppose that $|G| = 105$. If G has a normal Sylow 3-subgroup, prove that it must lie in the center of G.

47 Let G and H be the cyclic groups of order n and k respectively. Prove that the number of homomorphisms from G to H is the sum of all $\varphi(d)$, where d runs over all common divisors of n and k, and φ denotes the Euler φ function.

48 Let R be the ring of all n by n matrices with integer entries. Prove that the matrix $A \in R$ is invertible if and only if its determinant is ± 1.

49 Using Zorn's Lemma, prove that each non-zero commutative ring with an identity has maximal ideals.

50 Using Zorn's Lemma, prove that in each non-zero commutative ring with identity, minimal prime ideals exist.

51 Consider $A = \mathbb{R}^{\mathbb{N}}$, the ring of all real valued sequences, under pointwise operations. Prove:

(a) For each $n \in \mathbb{N}$, $M_n = \{f(n) = 0\}$ is a maximal ideal of A;

(b) There exist maximal ideals besides the M_n ($n \in \mathbb{N}$). Use Zorn's Lemma.

52 Suppose that A is a commutative ring with identity. Suppose that $a \in A$ is not nilpotent. Prove that there is a prime ideal that fails to contain a. Use this to show that the set of all nilpotent elements of A is the intersection of all prime ideals of A.

53 Let F be a field, and $A = F[[x]]$ denote the ring of formal power series in one variable. Prove the following:

(a) The units of A are precisely the power series whose constant term is nonzero.

(b) Suppose that $k \geq 1$ is an integer. Let I_k denote the set of all power series $\displaystyle\sum_{n=0}^{\infty} a_n x^n$ for which $a_0, \ldots, a_{k-1}$ are all zero. Each I_k is an ideal of A.

(c) If J is a nonzero proper ideal of A, then $J = I_m$, for some $m \geq 1$.

54 Prove the Division Algorithm for the ring $\mathbb{Z}[i]$ of Gaussian integers.

55 Let D be an integer which is not a square in $\mathbb{Z}$. Consider the subring $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$; (do not prove it is a subring.) Define $N(a + b\sqrt{D}) = a^2 - Db^2$. Assume that $N(xy) = N(x)N(y)$, for all $x, y \in \mathbb{Z}[\sqrt{D}]$. Prove that

(a) $a + b\sqrt{D}$ is a unit of $\mathbb{Z}[\sqrt{D}]$ if and only if $N(a + b\sqrt{D}) = \pm 1$.

(b) If $D < -1$, prove that the units of $\mathbb{Z}[\sqrt{D}]$ are precisely ± 1.

56 A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Prove:

(a) Every boolean ring has characteristic 2 and is commutative.

(b) Assume R is a boolean ring. Prove that every prime ideal is maximal.

57 A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Assume the preceding exercise. Use the Chinese Remainder Theorem to prove that every finite boolean ring has 2^n elements, for a suitable non-negative integer n.

58 Suppose that A is a nonzero commutative ring with identity. Let $n(A)$ denote the set of nilpotent elements of A; you may assume here that it is an ideal. Prove the equivalence of the following three statements:

(a) Every nonunit of A is nilpotent.

(b) $A/n(A)$ is a field.

(c) A has exactly one prime ideal.

59 Prove the Chinese Remainder Theorem: if A is a commutative ring with identity, and I and J are comaximal ideals of A, then $IJ = I \cap J$, and the homomorphism $\varphi : A \to A/I \times A/J$ defined by $\varphi(a) = (a + I, a + J)$ is surjective.

60 Let D be an integral domain. Prove that the ring $D[T]$ of polynomials over D in one indeterminate is a principal ideal domain if and only if D is a field.

61 Let A be a commutative ring with 1. Suppose that I and J are ideals of A. Prove that:

(a) Prove that $IJ \subseteq I \cap J$, and given an example where equality does not hold.

(b) Suppose that A is the (ring) direct product of two fields. Show that $IJ = I \cap J$, for any two ideals I and J of A.

62 Suppose that D is an integral domain. A polynomial $f(x)$ over D is *primitive* if the greatest common divisor of its coefficients is 1.

Prove the following form of Gauss' Lemma: If D is a unique factorization domain, then the product of any two primitive polynomials over D is primitive.

63 Let A be an integral domain, and P be a prime ideal of A. Define A_P to be the subset of the quotient field K of A, consisting of all fractions whose denominator is not in P. Prove that

(a) A_P is a subring of K;

(b) A_P has exactly one maximal ideal; identify it.

64 (a) Define *Euclidean Domain* and *Principal Ideal Domain*.

(b) Prove that any Euclidean Domain is a Principal Ideal Domain.

65 Convince that the polynomial rings $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ have the same field of fractions, but the power series rings $\mathbb{Z}[[X]]$ and $\mathbb{Q}[[X]]$ do not.

66 Consider the polynomial X^2+1 over the field $\mathbb{Z}/7\mathbb{Z}$. Prove that $E = (\mathbb{Z}/7\mathbb{Z})[X]/(X^2+1)$ is a field of 49 elements.

67 Let n be a natural number; prove that the polynomial

$$\Phi_n(X) := \frac{X^n - 1}{X - 1}$$

is irreducible over the ring $\mathbb{Z}$ precisely when n is prime.

68 Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

69 Give examples of the following, and justify your choices:

(a) A unique factorization domain which is not a principal ideal domain.

(b) A local integral domain with a *nonzero* prime ideal that is not maximal.

(c) An integral domain in which the uniqueness provision of "unique factorization" fails.

70 Suppose that F is a field and G is a multiplicative subgroup of $F \setminus \{0\}$. Prove that G is cyclic.

71 Suppose that F is a field and $q(x) := a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ is an irreducible polynomial in $F[x]$. Prove that $E = F[x]/(q(x))$ is a field which is an n dimensional vector space in F.

72 Let R be a ring with identity and M be an R-module. An element $x \in M$ is called a *torsion element* if $rx = 0$ for some nonzero $r \in R$. Let $T(M)$ denote the subset of all torsion elements of M.

(a) If R is an integral domain, show that $T(M)$ is a submodule of M.

(b) Give an example to show that $T(M)$ in general is not a submodule of M.

73 Suppose that A is a commutative ring with identity, and I is an ideal of A.

(a) For each positive integer n, prove that

$$A^n/IA^n \cong A/I \times \cdots A/I.$$

(b) Use (a) to prove that if $A^m \cong A^n$, where m and n are positive integers, then $m = n$. (You may use the corresponding fact for fields.)

74 Prove that $\mathbb{Q}$, the additive group of the rationals, is not a free abelian group.

75 Suppose that G is an abelian group, generated by x_1, x_2, x_3, x_4, and subject to the relations:

$$4x_1 - 2x_2 - 2x_3 = 0, \quad 8x_1 - 12x_3 + 20x_4 = 0, \quad 6x_1 + 4x_2 - 16x_4 = 0.$$

Write G as a direct product of cyclic groups.

76 Let R be a commutative ring with identity. If F is a free R-module of rank $n < \infty$, show that $\mathrm{Hom}_R(F, M) \cong M^n$ for each R-module M.

77 Let V be a vector space over the field F. Suppose that U_1 and U_2 are finite dimensional subspaces of V. Prove that $\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

78 Suppose that $T : V \to W$ is a linear transformation between vector spaces over the same field F. Prove that T is one-to-one precisely when it maps linearly independent sets to linearly independent sets.

79 Suppose that $T : V \to V$ is a linear transformation on the vector space V. Call T a *projection* if $T^2 = T$. Prove that if T is a projection then $V = \mathrm{Ker}(T) \oplus \mathrm{Im}(T)$. Give an example to show that the converse is false.

80 Suppose that V is a finite dimensional vector space over the field F and that $T : V \to W$ is a linear transformation into a vector space W over F. Prove that

$$\dim(V) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T)).$$

81 Obtain a formula for the number of one dimensional subspaces of an n dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$ of p elements (where p is a prime number). Justify your choice.

82 (a) Define: *Irreducible module* over a ring R with identity.

(b) Now assume that R is commutative as well. Prove that the R-module M is irreducible if and only if $M \cong R/I$ for some maximal ideal I of R. Use this to classify the irreducible $\mathbb{Z}$-modules.

83 Prove **Schur's Lemma**: Suppose that M is an irreducible module; then every nonzero endomorphism of M is an automorphism. Show how one concludes from this that if M is irreducible then $\mathrm{End}(M)$ is a division ring.

84 Let R be a ring with identity. Suppose that $\varphi : M \to F$ is a surjective R-module homomorphism and that F is a free R-module. Prove that $M = \mathrm{Ker}\,\varphi \oplus N$, where $N \cong F$.

85 Let R be a principal ideal domain and M be a torsion R-module. Define *primary module* and prove that M is isomorphic to a direct sum of primary R-modules.

86 Suppose that V is a finite dimensional vector space over the field F and that T is a linear transformation on V, so that the induced module action of $F[x]$ on V defines a cyclic module with cyclic vector w. Prove that:

(a) The set $\{w, T(w), T^2(w), \ldots, T^k(w)\}$ is a basis for a suitable k.

(b) Compute the matrix of T relative to this basis, pointing out the relationship which the entries of this matrix and k have to the monic polynomial in $F[x]$ that generates the annihilator of w.

(c) Compute the characteristic polynomial of the matrix in (b).

87 Suppose that T is a linear transformation on a finite dimensional vector space V, over a field F. Prove that T is diagonalizable if and only if $m_T(x)$, the minimum polynomial of T, can be factored as

$$m_T(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k),$$

where the $\lambda_i \in F$ $(i = 1, \ldots, k)$ are distinct.

88 Suppose that A is a nilpotent 6×6 matrix over a field. Find all possible Jordan Canonical forms of A. Justify your arguments.

89 Prove that in $GL_2(\mathbb{Q})$ all the elements of order four are conjugate. (Hint: Consider the rational canonical form of such an element.)

90 Suppose that V is a vector space of dimension 7 over the field of real numbers $\mathbb{R}$, and T is a linear transformation on V which satisfies $T^4 = I$. Compute the following:

(a) the possible minimum polynomials of T, and the characteristic polynomial that goes with each choice,

(b) the possible Rational Canonical Forms of T.

91 Suppose that V is a finite dimensional vector space over $\mathbb{Q}$, and T is an invertible linear transformation on V for which $T^{-1} = T^2 + T$. Prove:

(a) The dimension of V is a multiple of 3.

(b) If the dimension is 3, prove that all such transformations are similar.

92 Consider the statement:

All 3×3 matrices $A \neq I$ with real entries, such that $A^3 = I$ are similar over $\mathbb{R}$.

Prove or disprove.

93 Prove, over any field F, that if two 2×2 matrices or two 3×3 matrices have the same minimum and characteristic polynomials then they are similar matrices. Give an example which shows that this is false for matrices of greater dimension.

94 On a vector space V of dimension 8 over the field $\mathbb{Q}$, T is a linear transformation for which the minimum polynomial is

$$m_T(x) = (x^2 + 1)^2(x - 3).$$

Determine all possible Rational Canonical Forms. Justify your answer.

95 A *projection* is a linear transformation $P : V \to V$ on a vector space V for which $P^2 = P$. Assume that V has finite dimensional and prove the following:

(a) Any projection is diagonalizable.

(b) Two projections have the same diagonal form if and only if their kernels have the same dimension.

96 Prove that there are exactly two conjugacy classes of 5×5 matrices with entries in $\mathbb{Q}$ for which $T^8 = 1$ and $T^4 \neq 1$.

97 T is a linear transformation on the n dimensional vector space V, over the field G, and there is a basis $\{v_1, \ldots, v_n\}$ for V for which $T(v_i) = v_{i+1}$, for $i = 1, 2, \ldots, n-1$ and $T(v_n) = v_1$. As a module over $F[x]$ with the action induced by T, show that

(a) V is a cyclic module but not irreducible.

(b) If $F = \mathbb{Q}$ and n is a prime number, prove that V is the direct sum of two irreducible $F[x]$-submodules, of dimensions 1 and $n-1$, respectively, over $\mathbb{Q}$.

98 (a) Define the terms *eigenvector* and *eigenvalue* of a linear transformation T.

(b) Prove that the set of eigenvectors of T for which the corresponding eigenvalues are distinct must be linearly independent.

99 Find one representative of each conjugacy class of elements of order 2 in the group $GL_5(\mathbb{F}_2)$ of invertible 5×5 matrices with entries in the field of two elements.

100 Let $GL_4(\mathbb{F}_3)$ denote the group of all invertible 4×4 matrices with entries in $\mathbb{F}_3$, the field of three elements. Use rational canonical forms to determine the number of conjugacy classes of elements of order 4. Give the rational canonical form for each class.

101 Over $\mathbb{Q}$, compute the Jordan canonical form J of

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

Then, find a matrix S such that $J = SAS^{-1}$.

102 Over $\mathbb{Q}$, consider the following matrix:

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

Answer the following:

(a) Prove that A is diagonalizable.

(b) Is the $\mathbb{Q}[T]$-module structure on $\mathbb{Q}^4$ by A, via $f(T) \cdot v = f(A)v$, cyclic? Explain.

103 Let $\mathbb{C}$ be the field of complex numbers. Prove that each irreducible $\mathbb{C}[T]$-module is isomorphic to $\mathbb{C}$.

104 Prove that if F is a finite field, then there is a prime number p and a natural number n such that F has p^n elements.

105 Suppose that F is a subfield of K and K a subfield of L, so that the dimensions $\big[K : F\big]$ and $\big[L : K\big]$ are finite. Prove that $\big[L : F\big]$ is also finite and that

$$\big[L : F\big] = \big[L : K\big]\big[K : F\big].$$

106 Determine the dimension over $\mathbb{Q}$ of the extension $\mathbb{Q}\left(\sqrt{3+2\sqrt{2}}\right)$. Justify your arguments.

107 Prove that $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Conclude that $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 4$, and find a monic irreducible polynomial over $\mathbb{Q}$ satisfied by $\sqrt{3}+\sqrt{5}$.

108 Suppose that F is a field whose characteristic is not 2. Assume that $d_1, d_2 \in F$ are not squares in F. Prove that $F\left(\sqrt{d_1},\sqrt{d_2}\right)$ is of dimension 4 over F if $d_1 d_2$ is not a square in F and of dimension 2 otherwise.

109 Suppose that $[F(\alpha) : F]$ is odd; prove that $F(\alpha) = F(\alpha^2)$.

110 Let L be a field extension of F. Prove that the subset E of all elements of L which are algebraic over F is a subfield of L containing F.

111 Determine the splitting field of $x^4 - 2$ over $\mathbb{Q}$. It suffices to describe it as the subfield of $\mathbb{C}$, the field of complex numbers, generated by certain well-identified elements. Justify your choices.

112 Suppose that F is a field. For $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, define the *derivative* $D_x f(x)$ by

$$D_x[f(x)] = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

Prove the following: In a splitting field of $f(x)$, u is a multiple root of $f(x)$ if and only if u is a root of both $f(x)$ and $D_x f(x)$.

113 Assume the existence and uniqueness, up to isomorphism, of the splitting of a polynomial over an arbitrary base field. Let p be a prime number. Now consider the polynomial $x^{p^n} - x$ over the field $\mathbb{F}_p$ of p elements. Let K_{p^n} be its splitting field. Prove that K_{p^n} has p^n elements. Now consider any field $\mathbb{F}$ having p^n elements and prove that $\mathbb{F} \cong K_{p^n}$.

1.2 Groups

1 State and prove Cayley's Theorem about finite groups.

Cayley's Theorem:

Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.

Proof:

Let $g \in G$ be arbitrary. Consider the function $f_g : G \to G$ defined by $f_g(x) = g \cdot x$. Since G is a group, g has a two-sided inverse g^{-1}. Thus, the function f_g has a two-sided inverse $f_{g^{-1}}$, and so f_g is a bijection from G to G. Therefore, we may view f_g as a permutation of G.

We now show that $\mathcal{S} := \{f_g \mid g \in G\}$ is a subgroup of S_n which is isomorphic to G. Consider the function $\Phi : G \to S_n$ defined by $\Phi(g) = f_g$. Firstly, Φ is a homomorphism, since

$$\Phi(gh) = f_{gh} = [x \mapsto gh \cdot x] = [x \mapsto g \cdot hx] = [x \mapsto gx] \circ f_h = f_g \circ f_h = \Phi(g)\Phi(h).$$

Additionally, Φ is injective since if $f_g = f_h$, then $f_g(1) = f_h(1)$ and so $g = h$.

Thus, by the **First Isomorphism Theorem**, $G \cong \Phi(G)$, and by construction $\Phi(G) = \mathcal{S}$. Hence $\mathcal{S} \leq S_n$ and $G \cong \mathcal{S}$. $\square$

2 (a) Compute the order of the general linear group $GL_n(\mathbb{Z}_p)$, with p a prime number.

(b) Calculate the order of the subgroup $SL_n(\mathbb{Z}_p)$ of matrices which have determinant 1.

Proof of (a):

Consider the possibilities of a matrix $A \in GL_n(\mathbb{Z}_p)$. It must be true that A is invertible, and so no column of A is a linear combination of any of the other columns. The first column can be any nonzero vector, and thus there are $p^n - 1$ possibilities. The second column can be any vector that is not a multiple of the first column (note that the zero vector) is the zero multiple of the first column. So, there are $p^n - p$ possibilities for the second column.

The third column can be any vector that is not a linear combination of the first two vectors. Hence, there are $p^n - p^2$ possibilities for the third columns. Following this pattern, there are $p^n - p^{n-1}$ possibilities for the n^{th} column. Thus,

$$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) = \prod_{i=0}^{n-1} (p^n - p^i). \ \square$$

Proof of (b):

Consider the function $\Phi : GL_n(\mathbb{Z}_p) \to (\mathbb{Z}_p)^\times$ defined by $\Phi(A) := \det(A)$. Now, observe that $\operatorname{Ker} \Phi = SL_n(\mathbb{Z}_p)$. So

$$|SL_n(\mathbb{Z}_p)| = \frac{|GL_n(\mathbb{Z}_p)|}{|(\mathbb{Z}_p)^\times|} = \frac{|GL_n(\mathbb{Z}_p)|}{p-1} = \frac{1}{p-1} \prod_{i=0}^{n-1} (p^n - p^i). \ \square$$

3 (a) Prove that two elements of the symmetric group S_n are conjugate if and only if their cycle types are the same.

(b) Is this true for the alternating groups? Justify your answer.

Proof of (a):

Lemma: Any two m-cycles are conjugate in S_n.
Proof:

Let $\sigma := (s_1 \ \ s_2 \ \ \cdots \ \ s_m)$, and let $\tau := (t_1 \ \ t_2 \ \ \cdots \ \ t_m)$, such that $\sigma, \tau \in S_n$. Let $\pi \in S_n$ be such that $\pi(s_i) = t_i$ for all $i \in \{1, \ldots, m\}$. This assignment is a valid permutation because no two s_i map to the same t_i (as each t_i is unique), and the map is well-defined since each s_i is unique.

Now, $\pi\sigma\pi^{-1} = \pi(s_1 \ \ s_2 \ \ \cdots \ \ s_m)\pi^{-1} = (\pi(s_1) \ \ \pi(s_2) \ \ \cdots \ \ \pi(s_m)) = (t_1 \ \ t_2 \ \ \cdots \ \ t_m) = \tau$. Thus, σ and τ are conjugate. □

($\Longleftarrow$):

Let σ and τ have the same cycle type $(m_1, m_2, \ldots, m_k)$. Let σ be written by its cycle decomposition as $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$, where each σ_i is a m_i-cycle. Let τ be written by the same decomposition, with $\tau = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$, each τ_i being an m_i-cycle. Now, let $\pi := \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$, where π_i conjugates σ_i to τ_i. This exists by the **Lemma**.

Computing,

$$\begin{aligned} \pi\sigma\pi^{-1} &= (\pi_1\sigma_1\pi_1^{-1}) \circ \cdots \circ (\pi_k\sigma_k\pi_k^{-1}) \qquad (\dagger) \\ &= (\pi_1\sigma_1\pi_1) \circ \cdots \circ (\pi_k\sigma_k\pi_k) \\ &= \tau_1 \circ \cdots \circ \tau_k \\ &= \tau \end{aligned}$$

Step (†) is true since any integers in σ_1 and π_1 do not appear in another σ_i or π_i. Thus, σ and τ are conjugate. □

($\Longrightarrow$):

Let σ and τ be conjugate in S_n. Let $\pi \in S_n$ be such that $\pi\sigma\pi^{-1} = \tau$. Let σ be written in its cycle decomposition form as $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$.

Now, $\tau = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$, where $\tau_i = \pi\sigma_i\pi^{-1}$, and thus τ_i and σ_1 are cycles of the same length. Thus τ and σ have the same cycle type. □

Proof of (b):

The assertion holds in only one direction in the alternating groups. It is still true that is two permutations are conjugate, than they must have the same cycle type. The above proof holds.

However, the converse is false. Consider the permutation $\sigma := (1\ 2\ 3\ 4\ 5) \in A_5$. Note that the order of the conjugacy class of σ in S_5 is 24. So, the centralizer of σ in S_5 (denoted from now on as $C_{S_5}(\sigma)$ has order $120/24 = 5$ by the **Orbit-Stabilizer Theorem**. Since $C_{A_5}(\sigma) \leq C_{S_5}(\sigma)$, and $C_{A_5}(\sigma)$ is nontrivial, we have that $|C_{A_5}(\sigma)| = 5$. Therefore, by the **Orbit-Stabliizer Theorem**, the orbit of σ in A_5 has order $60/5 = 12$. Since there are 24 5-cycles in A_5, we see that they are divided into two separate conjugacy classes, even though they all have the same cycle type. □

4 Prove that if $|G| = 12$ and G has 4 Sylow 3-subgroups, then $G \cong A_4$.

Proof:

Consider the function $\varphi : G \to S_4$ that sends an element to the permutation of its action on the 4 Sylow-3 subgroups. Let $P \in \mathrm{Syl}_3(G)$. Since $n_3 = 4$, we have $|G : N_G(P)| = n_3 = 4$. Thus, $|N_G(P)| = 3$, and since $P \leq N_G(P)$, we have that $N_G(P) = P$. Consider $\mathrm{Ker}\,\varphi$ which consists of the elements that normalize every Sylow 3-subgroup. Certainly $\mathrm{Ker}\,\varphi \leq P$. So, either $\mathrm{Ker}\,\varphi = 1$ or $\mathrm{Ker}\,\varphi = P$. Since P is not normal, we have $\mathrm{Ker}\,\varphi = 1$. Thus φ is injective and so $G \cong \varphi(G)$.

Each of the 4 Sylow 3-subgroups has two elements of order three, and so the group G has eight elements of order 3, as does S_4. These eight elements are all even permutations. So, $|G \cap A_4| \geq 8$. Since $|\varphi(G)| = 12$, we must have that the subgroup of S_4 containing these eight even permutations is A_4. Thus $G \cong A_4$. □

5 Let p and q be prime numbers, and suppose that $p < q$. If G is a group of order pq and p does not divide $q - 1$, show that G must be cyclic.

Proof:

By **Sylow's Theorem**, $n_q \equiv 1 \bmod q$ and $n_q \mid p$. Since $p < q$, we have $n_q = 1$. Let $Q \in \mathrm{Syl}_q(G)$.

By **Sylow's Theorem**, $n_p = 1 + pm$, for some $m \in \mathbb{N}$, and $n_p \mid q$. If $n_p \neq 1$, then since q is prime, we must have $n_p = q$. Then, $q = 1 + pm$ and so $q - 1 = pm$, which contradicts the assumption that $p \nmid q - 1$. So, $n_p = 1$. Let $P \in \mathrm{Syl}_p(G)$.

Since $P \cap Q = 1$, we can write G as a semidirect product of P and Q. Because $P \trianglelefteq G$ and $Q \trianglelefteq G$, we have that the semidirect product between the two subgroups is actually the direct product $Z_p \times Z_q$. Because p and q are relatively prime, this group is cyclic and isomorphic to the cyclic group Z_{pq}. □

6 Recall that a group G is called a *p-group* (p a prime number) if for each $g \in G$, $g^{p^i} = 1$, for some positive integer i.

(a) Prove that if G is a finite p-group, then its center is not trivial.

(b) Use this fact to prove that every finite p-group is nilpotent.

Proof of (a):

Let G be a finite p-group. Recall the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(x_i)|,$$

where $x_1, \ldots, x_n$ are representatives for the conjugacy classes not contained in the center of G.

For any representative x_i, we have that $C_G(x_i) \leq G$. In addition, $C_G(x_i) \neq G$, since then we would have $x_i \in Z(G)$. Thus $|G : C_G(x_i)| > 1$, and so $p \mid |G : C_G(x_i)|$, for each i.

Because G is a p-group, $p \mid |G|$. By the class equation, since $p \mid |G|$ and $p \mid |G : C_G(x_i)|$ for each x_i, we must have $p \mid Z(G)$. Therefore, $|Z(G)| > 1$ and so G has a non-trivial center. □

Proof of (b):

A group G is nilpotent if it has an *upper central series* that terminates in the whole group G after finitely many steps. The upper central series for a group G is:

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots,$$

where $Z_0(G) = 1$, and $Z_1(G) = Z(G)$, and

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Let G be a finite p-group. Since G is finite, it suffices to show that each term $Z_{i+1}(G)$ is either strictly larger than $Z_i(G)$ or equal to G. Let $Z_i(G) \neq G$. Then, $G/Z_i(G)$ is a non-trivial p-group. Therefore, its center $Z(G/Z_i(G))$ is non-trivial by **part (a)**.

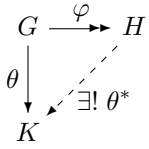
So, we have that the group $Z_{i+1}(G)/Z_i(G)$ is non-trivial. Thus, the group Z_{i+1} had order larger than $Z_i(G)$, by some power of p.

Now we have shown that the terms in the upper central series have strictly increasing group order, until the group is G itself. Thus the upper central series terminates in a finite number of steps, and so the finite p-group G is nilpotent. □

7 Suppose that $\varphi : G \to H$ and $\theta : G \to K$ are homomorphisms between groups. Assume that φ is surjective. Show that if $\mathrm{Ker}(\varphi)$ is contained in $\mathrm{Ker}(\theta)$ then there is a unique homomorphism $\theta^* : H \to K$ such that $\theta^* \circ \varphi = \theta$.

Proof:

We have the following diagram (the dashed line indicates the homomorphism that we're looking for):



Let $h \in H$. Pick $g \in G$ such that $\varphi(g) = h$. g exists since φ is surjective. Let $\theta^*(h) := \theta(g)$. (Note that this is well-defined.)

First we show that this θ^* is a homomorphism:

Let $\varphi(g_1) = h_1$, and $\varphi(g_2) = h_2$. Then, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$.

Therefore, $\theta^*(h_1)\theta^*(h_2) = \theta(g_1)\theta(g_2) = \theta(g_1 g_2) = \theta^*(h_1 h_2)$. Thus, θ^* is a homomorphism.

Lastly, we show that this homomorphism is unique:

Non-uniqueness is possible only in the following case:

$$\text{Given } h,\ \varphi(g_1) = \varphi(g_2) = h, \text{ but } \theta(g_1) \neq \theta(g_2).$$

In this case, $\varphi(g_1) = \varphi(g_2)$, so $\varphi(g_1 g_2^{-1}) = 1$. Hence, $\theta(g_1 g_2^{-1}) = 1$, and so $\theta(g_1) = \theta(g_2)$. Thus the case above is not possible. Therefore, the homomorphism θ^* is unique. □

8 Prove that if G is a finite group then any subgroup of index 2 is normal.

Proof:

By the definition of "index", there exist exactly two distinct left cosets of H:

$$H,\ gH,$$

where $g \in G \setminus H$.

Let $g_1, g_2 \in G \setminus H$. Now we show that $g_1 g_2 \in H$. Assume toward a contradiction that $g_1 g_2 \notin H$. Then,

$$\begin{aligned} g_1 g_2 H &= g_1 H \\ g_1 g_2 h_1 &= g_1 h_2, \text{ for some } h_1, h_2 \in H, \\ g_2 &= h_2 h_1^{-1} \in H, \end{aligned}$$

which is a contradiction. So, given $g_1, g_2 \in G \setminus H$, we have that $g_1 g_2 \in H$.

Now consider ghg^{-1} for some $g \in G$ and $h \in H$. There are two cases:

(**I**) If $g \in H$, then $ghg^{-1} \in H$ by multiplicative closure.

(**II**) If $g \notin H$, then $gh \notin H$, and $g^{-1} \notin H$, so by the above, we have $(gh)g^{-1} \in H$.

Thus, $H \trianglelefteq G$. □

9 Prove that any subgroup of a cyclic group is cyclic.

Proof:

Let $G = \langle x \rangle$. Let $H = \{1, x^{i_1}, x^{i_2}, \ldots\} \leq G$, with the set $\{i_1, i_2, \ldots\} \subseteq \mathbb{Z}$, and in no particular order. [Note that cyclic groups are necessarily countable in size.] Let $k := \gcd(\{i_\ell\}_{\ell=1}^{\ell=\infty})$.

Claim: $H = \langle x^k \rangle$. We show inclusion in both directions.

(**I**) $H \leq \langle x^k \rangle$:

Let $h \in H$, such that $h = x^{i_m}$ for some $m \in \mathbb{N}$. By construction, we have that $k \mid i_m$, so that $h = (x^k)^r$, where $rk = i_m$. Thus $H \leq \langle x^k \rangle$.

(**II**) $\langle x^k \rangle \leq H$:

Since $k = \gcd(\{i_\ell\}_{\ell=1}^{\ell=\infty})$, there exists $\{a_\ell\}_{\ell=1}^{\ell=\infty} \subseteq \mathbb{Z}$ such that $k = \sum a_\ell x^{i_\ell}$. Now we see that $x^k = (x^{i_1})^{a_1}(x^{i_2})^{a_2} \cdots$, and thus $x^k \in H$. So $\langle x^k \rangle \leq H$.

Thus $H = \langle x^k \rangle$.

Therefore, subgroups of cyclic groups are cyclic. □

10 Find all the automorphisms of order 3 in Z_{91}. (Hint: How can Z_3 act non-trivially on Z_{91}?) Does Z_{91} have any automorphisms of order 5? Explain.

Proof:

Note that $91 = 7 \cdot 13$, and by our study of groups of order pq, we know that $Z_{91} \cong Z_7 \times Z_{13}$. Thus, we have that $\mathrm{Aut}(Z_{91}) \cong \mathrm{Aut}(Z_7 \times Z_{13})$. Let $Z_7 \times Z_{13}$ be generated by the element $\{x\} \times \{y\}$.

An automorphism of a cyclic group is completely determined by where it sends x and y to. Since 7 and 13 are prime, we can send x to six different generators and y to twelve different generators. Thus $\mathrm{Aut}(Z_7 \times Z_{13}) \cong Z_6 \times Z_{12}$.

Now that we have this isomorphism, we can find the automorphisms of order 3 by identifying the elements of order 3 in $Z_6 \times Z_{12}$. Then Z_6 has two elements of order three corresponding to the automorphisms $[x \mapsto x^2]$ and $[x \mapsto x^4]$, and Z_{12} also has two elements of order three corresponding to the automorphisms $[y \mapsto y^3]$ and $[y \mapsto y^9]$.

Thus, the number of automorphisms of order 3 is 8: all combinations of the identity or automorphisms of order three gives us 9 automorphisms, and we subtract the identity automorphism which has order 1, leaving us with $9 - 1 = 8$ automorphisms of order 3.

On $Z_7 \times Z_{13}$ these are the automorphisms:

$$\begin{aligned}
(x, y) &\longmapsto (x, y^3) \\
(x, y) &\longmapsto (x, y^9) \\
(x, y) &\longmapsto (x^2, y) \\
(x, y) &\longmapsto (x^2, y^3) \\
(x, y) &\longmapsto (x^2, y^9) \\
(x, y) &\longmapsto (x^4, y) \\
(x, y) &\longmapsto (x^4, y^3) \\
(x, y) &\longmapsto (x^4, y^9)
\end{aligned}$$

To find the correspondence between these automorphisms of $Z_7 \times Z_{13}$ and the automorphisms of Z_{91}, we pick a generator a such that $Z_{91} = \langle a \rangle$, and solve the congruences

$$\left\{ \begin{array}{l} m \equiv i \bmod 7 \\ m \equiv j \bmod 13 \end{array} \right\},$$

for $i \in \{1, 2, 4\}$, $j \in \{1, 3, 9\}$, and i, j both not 1. Then, each m gives us an automorphism of Z_{91} $[a \mapsto a^m]$ which has order 3. The solutions are:

$$\left\{ \begin{array}{l} m \equiv 1 \bmod 7 \\ m \equiv 3 \bmod 13 \end{array} \right\} \implies m = 29$$

$$\left\{ \begin{array}{l} m \equiv 1 \bmod 7 \\ m \equiv 9 \bmod 13 \end{array} \right\} \implies m = 22$$

$$\left\{ \begin{array}{l} m \equiv 2 \bmod 7 \\ m \equiv 1 \bmod 13 \end{array} \right\} \implies m = 79$$

$$\left\{ \begin{array}{l} m \equiv 2 \bmod 7 \\ m \equiv 3 \bmod 13 \end{array} \right\} \implies m = 16$$

$$\left\{ \begin{array}{l} m \equiv 2 \bmod 7 \\ m \equiv 9 \bmod 13 \end{array} \right\} \implies m = 9$$

$$\left\{ \begin{array}{l} m \equiv 4 \bmod 7 \\ m \equiv 1 \bmod 13 \end{array} \right\} \implies m = 53$$

$$\left\{ \begin{array}{l} m \equiv 4 \bmod 7 \\ m \equiv 3 \bmod 13 \end{array} \right\} \implies m = 81$$

$$\left\{ \begin{array}{l} m \equiv 4 \bmod 7 \\ m \equiv 9 \bmod 13 \end{array} \right\} \implies m = 74$$

So, the automorphisms of order 3 in $Z_{91} = \langle a \rangle$ are:

$$a \longmapsto a^9$$

$$a \longmapsto a^{16}$$

$$a \longmapsto a^{22}$$

$$a \longmapsto a^{29}$$

$$a \longmapsto a^{53}$$

$$a \longmapsto a^{74}$$

$$a \longmapsto a^{79}$$

$$a \longmapsto a^{81}.$$

However, there are no automorphisms of order 5, since $Z_6 \times Z_{12}$ has no elements of order 5. □

11 Suppose that G is a nonabelian group of order 21. Prove:

(a) $Z(G) = \{e\}$;

(b) G has an automorphism which is not inner.

Proof of (a):

Claim: If $G/Z(G)$ is cyclic, then G is abelian.

Since $G/Z(G)$ is cyclic, we can pick $g \in G$ such that $G/Z(G) = \langle\, gZ(G)\,\rangle$. Let $a, b \in G$ and write $aZ(G)$ as $g^iZ(G)$ and $bZ(G)$ as $g^jZ(G)$. So $a = g^ix$ and $b = g^jy$, for some $x, y \in Z(G)$.

Clearly x and y commute with everything, since they're in $Z(G)$, and we know g^i and g^j commute with each other. So,

$$\begin{aligned} ab &= g^ixg^jy, \\ &= g^ig^jxy, \\ &= g^jg^iyx, \\ &= g^jyg^ix, \\ &= ba. \end{aligned}$$

Thus, G is abelian. □

Now, we use the contrapositive of this statement: "If G is nonabelian, then $G/Z(G)$ is not cyclic." By assumption G is nonabelian, and so $G/Z(G)$ is not cyclic. Since $Z(G) \leq G$, it has order either 1, 3, 7, or 21 by Lagrange's Theorem.

Clearly $|Z(G)| \neq 21$, since G is nonabelian. If $|Z(G)| = 3$ or 7, then $|G/Z(G)| = 7$ or 3, and so $G/Z(G)$ cyclic, a contradiction. Thus, $|Z(G)| = 1$ and so $Z(G) = \{e\}$. □

Proof of (b):

Claim: $G/Z(G) \cong \text{Inn}(G)$:

Let $\Phi : G \to \text{Inn}(G)$ be defined by $\Phi(a) = \varphi_a$, where $\varphi_a : G \to G$ is conjugation by a, i.e., $\varphi_a(x) = axa^{-1}$.

This map is a homomorphism, since for all $x \in G$:

$$\begin{aligned}
[\Phi(ab)](x) &= \varphi_{ab}(x) \\
&= (ab)x(ab)^{-1} \\
&= abxb^{-1}a^{-1} \\
&= \varphi_a(bxb^{-1}) \\
&= \varphi_a(\varphi_b(x)) \\
&= (\varphi_a\varphi_b)(x) \\
&= [\Phi(a)\Phi(b)](x).
\end{aligned}$$

The map is also surjective, because each inner automorphism is (by definition) an automorphism which is conjugation by an element. Now,

$$\begin{aligned}
\text{Ker}\,\Phi &= \{a \in G \mid \varphi_a = \text{Id}\} \\
&= \{a \in G \mid axa^{-1} = x, \forall x\} \\
&= \{a \in G \mid ax = xa, \forall x\} \\
&= \{a \in G \mid a \in Z(G)\} \\
&= Z(G)
\end{aligned}$$

So, by the **First Isomorphism Theorem**, $G/Z(G) \cong \text{Im}(G) = \text{Inn}(G)$. $\square$

Now, since G has order 21, it has a normal Sylow 7-subgroup isomorphic to Z_7, so we can write G as some semidirect product $Z_7 \rtimes_\varphi Z_3$. Consider the embedding of this group into $\overline{G} := Z_7 \rtimes_\varphi Z_6$ (show that this exists!) by the inclusion map. So, G is a subgroup of index 2 in $\overline{G}$, and thus $G \trianglelefteq \overline{G}$. Let $g \in \overline{G} \setminus G$. Consider the function $f : G \to G$ with $f(x) := gxg^{-1}$. Since $G \trianglelefteq \overline{G}$, we do in fact have that $gxg^{-1} \in G$ for all $g \in \overline{G}$ and $x \in G$. Additionally, since $G \cong \text{Inn}(G)$ and $g \notin G$, we have that $f(x) \notin \text{Inn}(G)$. Therefore, the automorphism on G which is actually conjugation by g in $\overline{G}$ is an outer automorphism of G. $\square$

12 Let $GL_2(\mathbb{Z}_3)$ act on the four one-dimensional subspaces of $\mathbb{Z}_3^2$ by $g(\text{Span}\{v\}) = \text{Span}\{gv\}$, where $g \in GL_2(\mathbb{Z}_3)$ and $v \in \mathbb{Z}_3^2$. Prove that this action induces a surjective homomorphism of $GL_2(\mathbb{Z}_3)$ onto S_4 whose kernel is the subgroup of all scalar matrices.

Proof:

$$GL_2(\mathbb{Z}_3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \{0,1,2\},\ ad - bc \neq 0 \right\}.$$

$$\mathbb{Z}_3^2 = \left\{ \begin{Bmatrix} x \\ y \end{Bmatrix} \;\middle|\; x,y \in \{0,1,2\} \right\}.$$

The four one dimensional subspaces of $\mathbb{Z}_3^2$ are:

$$\text{Span}\left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\}, \quad \text{Span}\left\{ \begin{matrix} 1 \\ 0 \end{matrix} \right\}, \quad \text{Span}\left\{ \begin{matrix} 1 \\ 1 \end{matrix} \right\}, \quad \text{Span}\left\{ \begin{matrix} 1 \\ 2 \end{matrix} \right\}.$$

Now,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\text{Span}\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}\right) = \text{Span}\left\{\begin{pmatrix} b \\ d \end{pmatrix}\right\},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\text{Span}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\}\right) = \text{Span}\left\{\begin{pmatrix} a \\ c \end{pmatrix}\right\},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\text{Span}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}\right) = \text{Span}\left\{\begin{pmatrix} a+b \\ c+d \end{pmatrix}\right\},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\text{Span}\left\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right\}\right) = \text{Span}\left\{\begin{pmatrix} a+2b \\ c+2d \end{pmatrix}\right\} = \text{Span}\left\{\begin{pmatrix} a-b \\ c-d \end{pmatrix}\right\}.$$

Consider the homomorphism induced by this action: $\varphi : GL_2(\mathbb{Z}_3) \to S_4$. The kernel of this action is the subgroup of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_3)$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\text{Span}\left\{\begin{pmatrix} x \\ y \end{pmatrix}\right\}\right) = \text{Span}\left\{\begin{pmatrix} x \\ y \end{pmatrix}\right\}, \text{ for all } \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}_3^2.$$

Hence,

$$\begin{pmatrix} b \\ d \end{pmatrix} \in \text{Span}\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\} \tag{1}$$
$$\begin{pmatrix} a \\ c \end{pmatrix} \in \text{Span}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} \tag{2}$$
$$\begin{pmatrix} a+b \\ c+d \end{pmatrix} \in \text{Span}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\} \tag{3}$$
$$\begin{pmatrix} a-b \\ c-d \end{pmatrix} \in \text{Span}\left\{\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right\} \tag{4}$$

From (1) we have that $b = 0$. From (2) we have that $c = 0$. Thus from (3), it must be true that $a = d$. Hence, the kernel of φ is the set of (nonzero) scalar matrices, of which there are two. So, the image of φ has order $48/2 = 24$ by the **First Isomorphism Theorem**. Since the image of φ is a subgroup of S_4, we have that it must equal all of S_4. Hence the action is surjective. □

13 Let p be a prime number and n be a positive integer. Prove that the general linear group $GL_n(\mathbb{Z}_p)$ is isomorphic to the automorphism group of $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (n times).

Proof:

Let $\varphi \in \text{Aut}(\mathbb{Z}_p^n)$. Let $\{e_1, \ldots, e_n\}$ be a basis for vector space $\mathbb{Z}_p^n$. Then, φ is completely determined by to where it sends each e_i. Note that if $v_i := \varphi(e_i)$, then we must have that the set $\{v_i\}$ is linearly independent - otherwise $\text{Im}\,\varphi$ is a proper subset of $\mathbb{Z}_p^n$ and so φ is not an automorphism.

Let $\Phi : \text{Aut}(\mathbb{Z}_p^n) \to GL_n(\mathbb{Z}^p)$ be defined by $\Phi : \varphi \longmapsto \left(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}\right)$, where $\varphi : e_i \mapsto v_i$ and $\left(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}\right)$ is the $n \times n$ matrix with columns $\overrightarrow{v_i}$. By the discussion above, we in fact do have that $\text{Im}\,\varphi \subseteq GL_n(\mathbb{Z}^p)$, so this map is valid.

Let $\varphi, \psi \in \text{Aut}(\mathbb{Z}_p^n)$. Then, $\Phi(\varphi\psi) = \left(\overrightarrow{z_1}, \ldots, \overrightarrow{z_n}\right)$, where $\overrightarrow{z_i} := \varphi(\psi(e_i))$. Note that $\left(\overrightarrow{z_1}, \ldots, \overrightarrow{z_n}\right) = \left(\overrightarrow{v_1}, \ldots, \overrightarrow{v_n}\right) \cdot \left(\overrightarrow{w_1}, \ldots, \overrightarrow{w_n}\right)$, where $\overrightarrow{w_i} := \psi(e_i)$ and $\overrightarrow{v_i} := \varphi(\overrightarrow{w_i})$. Thus, $\Phi(\varphi\psi) = \Phi(\varphi)\Phi(\psi)$.

The map is surjective since any matrix in the general linear group represents a bijective linear transformation (i.e., an automorphism) on $\mathbb{Z}_p^n$. The map is injective because if the matrix representation is distinct, then some basis vector is sent to a different place, and so the automorphisms are different.

Hence Φ is a bijective homomorphism, and thus an isomorphism. Therefore, $GL_n(\mathbb{Z}_p) \cong \mathbb{Z}_p^n$. $\square$

14 Suppose that $\varphi : G \to H$ is a surjective homomorphism of groups. Prove the following about the assignment $\varphi^* : N \mapsto \varphi^{-1}(N)$. Assume that it maps subgroups to subgroups.

(a) φ^* is a bijection between the lattice of subgroups of H and the set of subgroups of G that contain $\mathrm{Ker}(\varphi)$.

(b) $N_1 \subseteq N_2$ if and only if $\varphi^*(N_1) \subseteq \varphi^*(N_2)$.

(c) $\varphi^*(N)$ is normal in G if and only if N is normal in H.

Proof of (a):

The first thing we show is that for any subgroup $H' \leq H$, we have that $\varphi^*(H')$ is a subgroup of G containing $\mathrm{Ker}(\varphi)$. We already have the assumption that $\varphi^*(H')$ is a subgroup of G (given in the question), so it remains to show that $\mathrm{Ker}(\varphi) \leq \varphi^*(H')$.

Let $g \in \mathrm{Ker}(\varphi)$. Then $\varphi(g) = e$. Since $e \in H'$, we have that $g \in \varphi^{-1}(H) = \varphi^*(H)$.
Thus $\mathrm{Ker}(\varphi) \leq \varphi^*(H')$.

Now, to show that φ^* is a bijection, we show that it's surjective and injective.

Surjective:

Let $G' \leq G$ with $\mathrm{Ker}(\varphi) \leq G'$. We want to find $H' \leq H$ such that $\varphi^*(H') = G'$.
Let $H' := \varphi(G')$. Then, $\varphi^*(H') = \varphi^*(\varphi(G')) = \varphi^{-1}(\varphi(G'))$.

Certainly $G' \leq \varphi^{-1}(\varphi(G'))$. We use that $\mathrm{Ker}(\varphi) \leq G'$ to show the reverse inclusion.

Let $g \in \varphi^{-1}(\varphi(G'))$. Then, $\varphi(g) \in \varphi(G')$.
Assume toward a contradiction that $g \notin G'$, even though $\varphi(g) \in \varphi(G')$.
Let $h = \varphi(g)$, where $h \in H$. Since $\varphi(G') = H'$, there exists $g' \in G'$ such that $\varphi(g') = h$.
So, we can pick $g' \in G'$ such that $\varphi(g') = \varphi(g)$.

Now,

$$\begin{aligned}
\varphi(g') &= \varphi(g),\\
\varphi(g')\varphi(g)^{-1} &= 1,\\
\varphi(g')\varphi(g^{-1}) &= 1,\\
\varphi(g'g^{-1}) &= 1,\\
g'g^{-1} &\in \mathrm{Ker}(\varphi),\\
g'g^{-1} &\in G',\\
g'g^{-1} &= \hat{g}, \text{ for some } \hat{g} \in G',\\
g' &= \hat{g}g,\\
g' &\in G'.
\end{aligned}$$

Thus, $\varphi^{-1}(\varphi(G')) \leq G'$, and so $\varphi^{-1}(\varphi(G')) = G'$. Therefore φ^* is surjective.

Injective:

Let $\varphi^*(H_1) = \varphi^*(H_2)$. That is, $\varphi^{-1}(H_1) = \varphi^{-1}(H_2)$.
So, $\{g \in G \mid \varphi(g) = H_1\} = \{g \in G \mid \varphi(g) = H_2\}$.
If $\varphi(g) \in H_1$, then $\varphi(g) \in H_2$, and vice versa. Therefore $H_1 = H_2$.

Thus, φ^* is a bijection. $\square$

Proof of (b):

($\Rightarrow$)

Let $N_1 \subseteq N_2$.
Let $g \in \varphi^*(N_1)$. Then, $\varphi(g) \in N_1$, and so $\varphi(g) \in N_2$ and thus $g \in \varphi^*(N_2)$. $\square$

($\Leftarrow$)

Let $\varphi^*(N_1) \subseteq \varphi^*(N-2)$.
Let $h \in N_1$. Then, there exists $g \in \varphi^*(N_1)$ such that $\varphi(g) = h$.
By assumption, $g \in \varphi^*(N_2)$, and this $\varphi(g) = h \in N_2$. $\square$

Proof of (c):

($\Rightarrow$)

Let $\varphi^*(N) \trianglelefteq G$.
Then,

$$\begin{aligned} g\varphi^*(N) &= \varphi^*(N)g, \\ g\varphi^{-1}(N) &= \varphi^{-1}(N)g, \\ \varphi(g\varphi^{-1}(N)) &= \varphi(\varphi^{-1}(N)g), \\ \varphi(g)N &= N\varphi(g). \end{aligned}$$

So, for $h \in H$, pick $g \in G$ such that $\varphi(g) = h$.
Then, as above, $hN = Nh$. Thus, $N \trianglelefteq H$. $\square$

($\Leftarrow$)

Let $N \trianglelefteq H$.

Assume toward a contradiction that $g\varphi^*(N) \neq \varphi^*(N)g$.
Then $\varphi(g\varphi^*(N)) \neq \varphi(\varphi^*(N)g)$.
Hence, $\varphi(g)N \neq N\varphi(g)$.
Since $\varphi(g) \in H$, this is a contradiction.

Thus, $\varphi^*(N) \trianglelefteq G$.

15 Let G be a finite group acting on the set S. Suppose that H is a normal subgroup of G so that for any $s_1, s_2 \in S$, there is a unique $h \in H$ so that $hs_1 = s_2$. For each $s \in S$, let $G_s = \{g \in G : gs = s\}$. Prove:

(a) $G = G_sH$, and $G_s \cap H = \{e\}$;

(b) if H is contained in the center of G, then G_s is normal and G is (isomorphic to) a direct product of G_S and H.

Proof of (a):

To show that $G = G_sH$, we need to show that for all $g \in G$, we can pick $k \in G_s$ and $h \in H$ such that $g = kh$. Since it's obvious that $G_sH \subset G$, we will then have equality. Pick $g \in G$ and $s \in S$. Let $t \in S$ be arbitrary. Since $g \cdot t \in S$, we can pick a unique $h_1 \in H$ such that $h_1 \cdot s = g \cdot t$ and a unique $h_2 \in H$ such that $s = h_2 \cdot t$. Now, for any $k \in G_s$:

$$\begin{aligned} g \cdot t &= h_1 \cdot s \\ &= h_1 \cdot (k \cdot s) \\ &= (h_1 k) \cdot s \\ &= (h_1 k) \cdot (h_2 \cdot t) \\ &= (h_1 k h_2) \cdot t \\ &= (k h_3 h_2) \cdot t \\ &= (kh) \cdot t. \end{aligned}$$

We used the fact that $H \trianglelefteq G$ to write $h_1 k = k h_3$ for some $h_3 \in H$, and we have $h := h_3 h_2 \in H$. So, $g \cdot t = (kh) \cdot t$ for all t, and hence $g = kh$, where $k \in G_s$ and $h \in H$. Since g was arbitrary, we conclude that $G = G_sH$.

To see that $G_s \cap H = \{e\}$, observe that $G_s \cap H = H_s$, and by the condition that there is a unique $h \in H$ such that $h \cdot s = s$, we have that $G_s \cap H = H_s = \{e\}$. $\square$

Proof of (b):

Let $H \subset Z(G)$. Then, $gh = hg$ for all $g \in G$ and $h \in H$.

Let $g \in G$ and let $\sigma \in G_s$. Let $h \in H$ and $k \in G_s$ be such that $kh = g$ (this exists by **part (a)**). Then,

$$\begin{aligned} g\sigma g^{-1} \cdot s &= (kh)\sigma(kh)^{-1} \cdot s \\ &= kh\sigma h^{-1}k^{-1} \cdot s \\ &= kh\sigma h^{-1} \cdot s \\ &= k\sigma h h^{-1} \cdot s \\ &= k\sigma \cdot s \\ &= s. \end{aligned}$$

Hence $g\sigma g^{-1} \in G_s$ and since g, σ were arbitrary, $G_s \trianglelefteq G$.

By **D&F Theorem 5.4.9**, since $H \trianglelefteq G$, $G_s \trianglelefteq G$ and $H \cap G_s = \{e\}$, we have that $G_sH \cong G_s \times H$, and so $G \cong G_s \times H$. $\square$

16 Suppose that G is a group and H is a proper subgroup of index k. Show that

(a) $g * (xH) = gxH$ defines a group action of G on the set $\Omega = (G/H)_\ell$ of left cosets of H;

(b) the kernel of the induced homomorphism into the permutation group on Ω is the intersection of all conjugates of H.

(c) Now suppose that G is simple and that $k > 1$ is the index of H. Then show that G is isomorphic to a subgroup of S_k.

Proof of (a):

In order for G to be acting on the left cosets of H, we need a map $G \times \Omega \to \Omega$ such that

(1) $g_1 * (g_2 * xH) = (g_1 g_2) * xH, \ \ \forall g_1, g_2 \in G, xH \in \Omega.$

(2) $1 * xH = xH, \ \ \forall xH \in \Omega.$

It's clear that the map given $[(g, xH) \longmapsto gxH]$ is in fact a map from $G \times A \to A$, where in this case $A = (G/H)_\ell$, since gxH is a left coset of H in G.

(1) The first property is true because:

$$\begin{aligned} g_1 * (g_2 * xH) &= g_1 * (g_2 xH) \\ &= g_1 g_2 xH \\ &= (g_1 g_2) xH \\ &= (g_1 g_2) * xH, \end{aligned}$$

by the properties of cosets.

(2) Again by the properties of cosets: $1 * xH = (1x)H = xH$.

Thus, the given map defines a group action of G on the set Ω. □

Proof of (b):

The kernel of the induced homomorphism into the permutation group on Ω is the set of all $g \in G$ such that $gxH = xH$ for all $xH \in \Omega$. We want to show that this is equal to the intersection of all conjugates of H. So, we wish to show the equality:

$$\{g \in G \mid gxH = xH, \ \forall xH \in \Omega\} \ = \ \bigcap_{g \in G} gHg^{-1}.$$

Let $gxH = xH$ for all $xH \in \Omega$, i.e., for all $x \in G$. Then,

$$\begin{aligned} gxH &= xH \\ gx &\in xH \\ g &\in xHx^{-1}. \end{aligned}$$

Therefore, g is in the intersection of all conjugates of H.

Let g be in the intersection of all conjugates of H. Then, for all $x \in G$,

$$\begin{aligned} g &\in xHx^{-1} \\ gx &\in H \\ gxH &= H. \end{aligned}$$

Therefore, $gxH = xH$, for all $x \in G$.

We have shown inclusion in both directions, and therefore the two sets are equal. □

Proof of (c):

Let G act on the k left cosets of H in G (note that the number of left cosets of a subgroup is equal to the the index of the subgroup in the whole group. As above, this is a valid group action. Since G is simple, the kernel of this action - which is necessarily a normal subgroup of G - must be either trivial or all of G. Since $k > 1$, the kernel is trivial. Therefore, by the **First Isomorphism Theorem**, $G \cong \text{Im}(G) \leq S_k$. □

17 Prove that a group of order 30 must have a normal subgroup of order 15.

Proof:

Let $|G| = 30 = 2 \cdot 3 \cdot 5$. By Sylow's Theorems, $n_3 \in \{1, 10\}$ and $n_5 \in \{1, 6\}$. Let $P \in \text{Syl}_3(G)$ and $Q \in \text{Syl}_5(G)$. Assume toward a contradiction that neither P nor Q is normal in G. Then, $n_3 = 10$ and $n_5 = 6$. So, G contains 20 elements of order 3 and 24 elements of order 5, which is clearly not possible. So, either $P \trianglelefteq G$ or $Q \trianglelefteq G$. By **D&F Corollary 3.1.15**, we have that $PQ \leq G$. Since $P \cap Q = \{e\}$, we have that $|PQ| = 15$. Recall that every subgroup of index 2 is normal, and therefore G has a normal subgroup of order 15. □

18 Classify the groups of order 70.

Proof:

By **Sylow's Theorem**:

$$n_2 \in \{1, 5, 7, 35\}$$
$$n_5 = 1$$
$$n_7 = 1$$

Let $P \in \text{Syl}_5(G)$ and $Q \in \text{Syl}_7(G)$. Since $n_5 = n_7 = 1$, we have that $P \trianglelefteq G$ and $Q \trianglelefteq G$, and hence $PQ \leq G$. Since $P \cap Q = \{e\}$ and $P \cong Z_5$ and $Q \cong Z_7$, the only possibility is that $PQ \cong Z_5 \times Z_7 \cong Z_{35}$.

Let $R \cong Z_2$. Now, to find all groups of order 70, we need to find all automorphisms $\varphi : R \to \text{Aut}(PQ)$ and determine up to isomorphism the groups $PQ \rtimes_\varphi R$.

If φ is an homomorphism from $R \cong Z_2$ to $\text{Aut}(PQ) \cong \text{Aut}(Z_{35}) \cong \text{Aut}(Z_5) \times \text{Aut}(Z_7) \cong Z_4 \times Z_6$, then of course $\varphi(e) = e$, and the automorphism is fully determined by which element of order two that we send the non-trivial $r \in R$ to. Note that Z_4 and Z_6 each have one element of order two. The element of order two in $\text{Aut}(Z_5)$ is $\varphi : x \mapsto x^4$, since $\varphi^2(x) = x^{16} = x$. The element of order two in $\text{Aut}(Z_7)$ is $\psi : y \mapsto y^6$, since $\psi^2(y) = y^{36} = y$. Thus, the elements of $\text{Aut}(PQ)$ of order two are:

$$\sigma_1 = (x, y) \longmapsto (x, y)$$
$$\sigma_2 = (x, y) \longmapsto (x^4, y)$$
$$\sigma_3 = (x, y) \longmapsto (x, y^6)$$
$$\sigma_4 = (x, y) \longmapsto (x^4, y^6)$$

Now, we can transform these from automorphisms on $Z_5 \times Z_7$ to automorphisms on Z_{35}. Solving

for the system:

$$\left\{ \begin{array}{l} m \equiv i \bmod 5 \\ m \equiv j \bmod 7 \end{array} \right\},$$

for $i \in \{1, 4\}$, $j \in \{1, 6\}$. The solutions are:

$$\left\{ \begin{array}{l} m \equiv 1 \bmod 5 \\ m \equiv 1 \bmod 7 \end{array} \right\} \implies m = 1$$

$$\left\{ \begin{array}{l} m \equiv 1 \bmod 5 \\ m \equiv 6 \bmod 7 \end{array} \right\} \implies m = 6$$

$$\left\{ \begin{array}{l} m \equiv 4 \bmod 5 \\ m \equiv 1 \bmod 7 \end{array} \right\} \implies m = 29$$

$$\left\{ \begin{array}{l} m \equiv 4 \bmod 5 \\ m \equiv 6 \bmod 7 \end{array} \right\} \implies m = 34$$

Hence, if $Z_{35} = \langle a \rangle$, then the automorphisms of order two are:

$$\widetilde{\sigma}_1 = a \longmapsto a$$
$$\widetilde{\sigma}_2 = a \longmapsto a^6$$
$$\widetilde{\sigma}_3 = a \longmapsto a^{29}$$
$$\widetilde{\sigma}_4 = a \longmapsto a^{34}$$

Hence, the possible homomorphisms $\varphi_i : R \to \mathrm{Aut}(PQ)$, for $r \in R$, are:

$$\varphi_1 = r \longmapsto \widetilde{\sigma}_1$$
$$\varphi_2 = r \longmapsto \widetilde{\sigma}_2$$
$$\varphi_3 = r \longmapsto \widetilde{\sigma}_3$$
$$\varphi_4 = r \longmapsto \widetilde{\sigma}_4$$

Of course $PQ \rtimes_{\varphi_1} R$ is the direct product $Z_{35} \times Z_2 \cong Z_{70}$. Writing each of the other three groups in semidirect product form:

$$G_2 := PQ \rtimes_{\varphi_2} R = \langle (k,h) \mid k \in PQ,\ h \in R,\ (k,h)(k',h') = (k[\varphi_2(h)](k'), hh') = \left\{ \begin{array}{ll} (kk', hh'), & h = e \\ (k(k')^6, hh'), & h \neq e \end{array} \right\} \rangle$$

$$G_3 := PQ \rtimes_{\varphi_3} R = \langle (k,h) \mid k \in PQ,\ h \in R,\ (k,h)(k',h') = (k[\varphi_3(h)](k'), hh') = \left\{ \begin{array}{ll} (kk', hh'), & h = e \\ (k(k')^{29}, hh'), & h \neq e \end{array} \right\} \rangle$$

$$G_4 := PQ \rtimes_{\varphi_4} R = \langle (k,h) \mid k \in PQ,\ h \in R,\ (k,h)(k',h') = (k[\varphi_4(h)](k'), hh') = \left\{ \begin{array}{ll} (kk', hh'), & h = e \\ (k(k')^{34}, hh'), & h \neq e \end{array} \right\} \rangle$$

So, there are at most four groups of order 70. Consider the these four groups of order 70: Z_{70}, $D_{14} \times Z_5$, $D_{10} \times Z_7$, D_{70}. We look at the number of elements of order two of each group (denoted $\mathbf{2}(G)$) to show none are pairwise isomorphic.

$$\mathbf{2}(Z_{70}) = 1$$
$$\mathbf{2}(D_{10} \times Z_7) = 5$$
$$\mathbf{2}(D_{14} \times Z_5) = 7$$
$$\mathbf{2}(D_{70}) = 35$$

So, these must be the four groups of order 70 up to isomorphism. □

19 Show that if G is a subgroup of S_n (n a natural number) containing an odd permutation, then half the elements of G are odd and half are even.

Proof:

Consider the sign function $\epsilon : S_n \to \{\pm 1\}$ where

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd} \end{cases}.$$

ϵ is a homomorphism because the product of two odd permutations or two even permutations is an even permutation, and the product of one odd and one even permutation is an odd permutation. If G contains an odd permutation σ, then $\mathrm{Im}\,(\epsilon\,|_G) = \{\pm 1\}$, since $\epsilon(\sigma) = -1$ and $\epsilon(e) = 1$. By the **First Isomorphism Theorem**, $|G/\operatorname{Ker}\epsilon| = |G|/|\operatorname{Ker}\epsilon| = |\{\pm 1\}| = 2$. So, there are two cosets $\{\operatorname{Ker}\epsilon,\ \sigma\operatorname{Ker}\epsilon\}$, each of which is the same size. Since $\operatorname{Ker}\epsilon$ contains exactly the even permutations in G, and $G = 2 \cdot |\operatorname{Ker}\epsilon|$, we have that G contains as many odd permutations as even permutations. □

20 Use #19 to prove that if G is a group of order $2m$, with m odd, then G cannot be simple, and, indeed, contains a subgroup of index 2.

Proof:

Let $P \in \mathrm{Syl}_2(G)$. Since m is odd, we have that $|P| = 2$ and there exists an element p of order 2.

Assume toward a contradiction that G is simple. Consider the map $\varphi : G \to S_{2m}$ defined by $\varphi(g) = \lambda_g$ where $\lambda_g : G \to G$ is defined by $\lambda_g : x \mapsto gx$ for all $x \in G$. Since G is simple, $\operatorname{Ker}\varphi$ must be trivial. Hence $G \cong \varphi(G) \subseteq S_{2m}$.

Now, for p as above, we have that $\lambda_p(x) = px$ and $\lambda_p(px) = p^2x = x$, for all x. Thus, λ_p contains a transposition for every two elements x, px, and hence λ_p is a product of m transpositions. Since m is odd, we have that λ_p is an odd permutation. By **Problem 19**, G contains half even permutations and half odd permutations. Since the set of even permutations forms a subgroup - which is now of index 2, and hence normal - we have that G is not simple, which is a contradiction.

Therefore, G is not simple, and G contains a subgroup of index 2. □

21 Classify the groups of order $4p$, where $p \geq 5$ is prime.

Proof:

First we consider the case where $p \equiv 3 \pmod 4$.

By Sylow's congruences, we have that $n_p \equiv 1 \pmod p$ and $n_p \mid 2$. Thus, $n_p = 1$. So for $H \in \mathrm{Syl}_p(G)$, necessarily $H \trianglelefteq G$. Similarly, we have that $n_2 \equiv 1 \bmod 2$ and $n_2 \mid p$. Hence, either $n_2 = 1$ or $n_2 = p$. If $n_2 = 1$, then for $K \in \mathrm{Syl}_2(G)$, we have that $K \trianglelefteq G$. In this case, we have that the group $G = HK \cong H \times K$ is abelian.

By the **Fundamental Theorem of Finitely Generated Abelian Groups**, either:

1) $G \cong \mathbb{Z}/4p\mathbb{Z}$, or

2) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2p\mathbb{Z}$.

Now assume that G is nonabelian. We consider the possible homomorphisms $\varphi : K \to \mathrm{Aut}(H)$. Since $|\operatorname{Aut}(H)| = p - 1$, and $p \equiv 3 \bmod 4$, we have that $2 \mid p$ and $4 \nmid p$. Note that $\mathrm{Aut}(H)$ is cyclic. Let a be the element of order 2 in $\mathrm{Aut}(H)$ (which exists since $\mathrm{Aut}(H)$ is cyclic and $2 \mid p - 1$.

If $K = \langle x \rangle \cong \mathbb{Z}/4\mathbb{Z}$, then the only possible homomorphism from K to $\mathrm{Aut}(H)$ is $\varphi : x \mapsto a$.

If $K = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then the possible homomorphisms map either $[(x,1) \mapsto a$ and $(1,y) \mapsto 1]$, or $[(x,1) \mapsto 1$ and $(1,y) \mapsto a]$ or $[(x,1) \mapsto a$ and $(1,y) \mapsto a]$. We must now determine if semidirect products with these homomorphisms yield isomorphic or non-isomorphic groups.

It is clear that the first two automorphisms are isomorphic, since they are identical up to switching the order of the pairs. Less obviously, the first and third homomorphisms differ (in the composition sense) by an automorphism of K. If φ_1 is the first map above and φ_3 is the third, then $\varphi_1 = \varphi_3 \circ \psi$, where $\psi((x,1)) = (x,1)$ and $\psi((1,y)) = (x,y)$. Therefore, all three of these homomorphisms yield pairwise isomorphic semidirect products.

So we have found the two nonabelian nonisomorphic semidirect products:

3) $G \cong H \rtimes_\varphi K$, with $K \cong \langle x \rangle \cong \mathbb{Z}/4\mathbb{Z}$, and φ maps x to an element of order 2 in $\mathrm{Aut}(H)$.

4) $G \cong H \rtimes_\psi K$, with $K \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $\psi = \varphi_1$ as above.

These are the four groups of order $4p$, with $p \equiv 3 \bmod 4$.

In the case where $p \equiv 1 \bmod 4$, we have that $4 \mid p-1$. Now, we can pick $a \in \mathrm{Aut}(H)$ with $|a| = 4$ since $\mathrm{Aut}(H)$ is cyclic and $4 \mid p-1$. For the case above where $K = \langle x \rangle \cong \mathbb{Z}/4\mathbb{Z}$, we have the two possible homomorphisms:

1) $\varphi_1 : x \mapsto a$,

2) $\varphi_2 : x \mapsto a^2$.

The semidirect products that arise from these two maps yield non-isomorphic groups because $\mathrm{Ker}\,\varphi_1 = \{e\} \neq \mathrm{Ker}\,\varphi_2$. So, this case has five groups of order $4p$. □

22 Let p be an odd prime number.

(a) Prove that in $GL_2(\mathbb{Z}_p)$ every element A of order 2, $A \neq -I$, is conjugate to the diagonal matrix U, for which $U_{1,1} = -1$ and $U_{2,2} = 1$.

(b) Now classify the groups of order $2p^2$, for which the Sylow p-subgroups are *not* cyclic.

Proof of (a):

First note that the only scalar matrix with order two is $-I$, since -1 is the only element with order 2 in $\mathbb{Z}_p$. We now show that an element of order 2 which is not equal to $-I$ is of one of the forms:

$$\pm 1 \cdot \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} \quad , \quad \pm 1 \cdot \begin{pmatrix} -1 & 0 \\ c & 1 \end{pmatrix}$$

Let $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ have order 2. Then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

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

$$\begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & bc+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\left\{ \begin{array}{c} a^2+bc = 1 \\ b(a+d) = 0 \\ c(a+d) = 0 \\ bc+d^2 = 1 \end{array} \right\}$$

Let $a + d \neq 0$. Then $b = c = 0$ since $\mathbb{Z}_p$ is an integral domain. So, $a^2 = d^2 = 1$ and so $a = \pm 1$ and $d = \pm 1$. Since $a + d \neq 0$, necessarily $a = -d$.

On the other hand, let $a + d = 0$. Factoring out a multiple, we can set $a = 1$ and $d = -1$, then we have that $bc = 0$ and so either $b = 0$ or $c = 0$.

Now, we find an element that conjugates $\begin{pmatrix} -1 & x \\ 0 & 1 \end{pmatrix}$ to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} -1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

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

$$\begin{pmatrix} -a + cx & -b + dx \\ c & d \end{pmatrix} = \begin{pmatrix} -a & b \\ -c & d \end{pmatrix}$$

From this, we get that $c = 0$, $b = dx \cdot 2^{-1}$, and a, d are arbitrary. We get a similar situation for the other case. Hence, in both cases, we can conjugate a matrix of order 2 to U. □

Proof of (b):

Let $|G| = 2p^2$. Let $P \in \mathrm{Syl}_p(G)$. Then, $|P| = p^2$, and by assumption, $P \ncong Z_{p^2}$, and therefore $P \cong Z_p \times Z_p$. (since all groups of order p^2 are abelian). We now seek to classify all semidirect products $(Z_p \times Z_p) \rtimes_\varphi Z_2$, for $\varphi : Z_2 \to \mathrm{Aut}(Z_p \times Z_p)$. Since $\mathrm{Aut}(Z_p \times Z_p) \cong GL_2(Z_p)$, we can find homomorphisms φ that map the nontrivial element of Z_2 to a matrix of order two. We can consider only one representative from each conjugacy class. So, we can map the nontrivial element of order two in Z_2, to either I, $-I$, or U.

In the first case, $G \cong Z_p \times Z_p \times Z_2$. In the second case, the nontrivial element of Z_2 inverts both components of $Z_p \times Z_p$ and so $G \cong D_{2p^2}$. In the third case, the nontrivial element of Z_2 inverts only one component, and so $G \cong D_{2p} \times Z_p$. These three are clearly nonisomorphic. □

23 (a) Prove that there are exactly four homomorphisms from Z_2 into $\mathrm{Aut}(Z_8)$.

(b) Show that these yield four pairwise nonisomorphic semidirect products.

Proof of (a):

First observe that Z_8 is cyclic, with a generator x. Automorphisms of Z_8 must map x to another generator. Z_8 has 4 generators: x, x^3, x^5, x^7. So, if $Z_2 = \langle y \rangle$, then possible homomorphism of Z_2 into $\mathrm{Aut}(Z_8)$ are:

$$\varphi_1 : y \longmapsto [x \mapsto x]$$

$$\varphi_2 : y \longmapsto [x \mapsto x^3]$$

$$\varphi_3 : y \longmapsto [x \mapsto x^5]$$

$$\varphi_4 : y \longmapsto [x \mapsto x^7]$$

These must be all homomorphisms. □

Proof of (b):

Now we consider the four semidirect products $Z_8 \rtimes_{\varphi_i} Z_2$, where φ_i is one of the four homomorphisms above.

$G_1 := Z_8 \rtimes_{\varphi_1} Z_2$ is the trivial semidirect product, i.e. the direct product $Z_8 \times Z_2$. This group is not isomorphic to the other three because this group is abelian and the other three are not

(nontrivial homomorphisms give nonabelian semidirect products). We now distinguish the other three groups by showing that the each have a different number of elements of order two.

Let $(h,k) \in G_2 := Z_8 \rtimes_{\varphi_2} Z_2$, with $k \neq e$. If $|(h,k)| = 2$, then

$$\begin{aligned}(h,k)^2 &= (1,1)\\ (h,k)(h,k) &= (1,1)\\ (h[\varphi(k)](h),1) &= (1,1)\\ (hh^3,1) &= (1,1)\\ h^4 &= 1.\end{aligned}$$

If $Z_8 = \langle x \rangle$ and $Z_2 = \langle y \rangle$, then the elements of order two in G_2 are:

$$(x^4,1) \quad (1,y) \quad (x^2,y) \quad (x^4,y) \quad (x^6,y)$$

Let $(h,k) \in G_3 := Z_8 \rtimes_{\varphi_3} Z_2$, with $k \neq e$. If $|(h,k)| = 2$, then

$$\begin{aligned}(h,k)^2 &= (1,1)\\ (h,k)(h,k) &= (1,1)\\ (h[\varphi(k)](h),1) &= (1,1)\\ (hh^5,1) &= (1,1)\\ h^6 &= 1.\end{aligned}$$

If $Z_8 = \langle x \rangle$ and $Z_2 = \langle y \rangle$, then the elements of order two in G_3 are:

$$(x^4,1) \quad (1,y) \quad (x^4,y)$$

Let $(h,k) \in G_4 := Z_8 \rtimes_{\varphi_4} Z_2$, with $k \neq e$. If $|(h,k)| = 2$, then

$$\begin{aligned}(h,k)^2 &= (1,1)\\ (h,k)(h,k) &= (1,1)\\ (h[\varphi(k)](h),1) &= (1,1)\\ (hh^7,1) &= (1,1)\\ h^8 &= 1.\end{aligned}$$

If $Z_8 = \langle x \rangle$ and $Z_2 = \langle y \rangle$, then the elements of order two in G_4 are:

$$\begin{array}{ccccc}(x^4,1) & (1,y) & (x,y) & (x^2,y) & (x^3,y)\\ (x^4,y) & (x^5,y) & (x^6,y) & (x^7,y) & \end{array}$$

Since each group has a different number of elements of order two, they are all nonisomorphic. □

24 Prove that S_4 contains no nonabelian simple groups.

Proof:

Since $|S_4| = 24$, any subgroup of S_4 will have order in $\{1,2,3,4,6,8,12,24\}$. For starters, any group of order $1, 2, 3$, or 4 is abelian.

The only group of order 6 which is nonabelian is S_3. There are four copies of S_3 embedded in S_4, but since $\langle (1\ 2\ 3) \rangle \trianglelefteq S_3$ (subgroup of index 2), S_3 is not simple.

The two groups of order 8 which are nonabelian are D_8 and Q_8. There are three copies of D_8 embedded in S_4, but since $\langle r \rangle \trianglelefteq D_8$ (subgroup of index 2), D_8 is not simple. There are no copies

of Q_8 in S_4. This is because Q_8 and S_4 both have 6 elements of order 4, and so if $Q_8 \leq S_4$, then Q_8 contains all the 4-cycles, and hence $Q_8 \ni (1\ 2\ 3\ 4)(1\ 3\ 4\ 2) = (1\ 4\ 3)$. But, since Q_8 has no elements of order 3, this is a contradiction. Therefore, $Q_8 \not\leq S_4$.

The only subgroup of order 12 in S_4 is A_4. A subgroup of A_4 is V_4, the Klein 4-group, which is normal in A_4 since it contains all the (2,2)-cycles, and conjugation does not change the cycle type. Hence, A_4 is not simple.

Lastly, S_4 itself is not simple, as it has a subgroup of index 2, namely A_4.

So, all subgroups of S_4 are either abelian, or not simple. Thus, S_4 contains no nonabelian simple groups. □

25 Use the result of **Exercise 24** to prove that if G is a nonabelian simple group, then every proper subgroup of G has index at least 5.

Proof:

Let G be a nonabelian simple group. Let $H \leq G$ with $|G : H| = k > 1$. Then, the action of G on the left cosets of H by left multiplication induces a homomorphism $\varphi : G \to S_k$. Since G is simple, $\operatorname{Ker}\varphi$ is either trivial or the whole group. However, if $\operatorname{Ker}\varphi = G$, then every element of G fixes all cosets of H in G, and since $|G : H| > 1$, this is not possible. Therefore, $\operatorname{Ker}\varphi = 1$ and thus by the **First Isomorphism Theorem**, we have that G is isomorphic to a subgroup of S_k. If $k \leq 4$, then $S_k \leq S_4$, and we showed in the previous exercise that S_4 has no nonabelian simple subgroups, this is a contradiction. Therefore, any proper subgroup of G has index at least 5. □

26 Prove that D_{2n} is nilpotent if and only if n is a power of 2. (Hint: Use the ascending central chain; recall that if there is an even number of vertices n, then $Z(D_{2n}) \neq \{e\}$.

Proof:

Lemma:

If G is nilpotent and $a, b \in G$, then $\big[\gcd(|a|, |b|) = 1 \implies ab = ba\big]$.

Proof:

Let G be nilpotent and let $a, b \in G$. Let $\gcd(|a|, |b|) = 1$. Since G is nilpotent, it is the internal direct sum of all the Sylow subgroups of G, so $G = P_1P_2 \cdots P_k$, where each P_i is a Sylow subgroup of G. So, $a = a_1 \cdots a_k$ and $b = b_1 \cdots b_k$, for $a_i, b_i \in P_i$. If $a_i \neq 1$, then $p_i \mid |a_i|$ and so $p_i \mid |a|$. Thus $p_i \nmid |b|$, and so $b_i = 1$. Similarly, if $b_i \neq 1$, then $a_i = 1$. So, renumbering the Sylow subgroups and combining, we can write G as $G \cong Q_1 \times Q_2$ where $a \in Q_1$ and $b \in Q_2$. Note that different p_i can be the same prime, but Q_1 and Q_2 cannot share any primes because then that prime divides both $|a|$ and $|b|$, which is a contradiction. Since $Q_1 \cap Q_2 = \{e\}$, we have that $ab = ba$. □

($\Rightarrow$)

Let D_{2n} be nilpotent. Assume toward a contradiction that $p \mid n$ for some odd prime p. Then, $r^{n/p} \in D_{2n}$ and $|r^{n/p}| = p$. Note that since $n/p \neq n/2$, we have that $r^{n/p} \neq r^{-n/p}$. But, by the above **Lemma**, $sr^{n/p} = r^{n/p}s$, and by multiplication in the dihedral group, $r^{n/p}s = sr^{-n/p}$, so $r^{n/p} = r^{-n/p}$, which is a contradiction. Therefore, n is a power of two. □

($\Leftarrow$)

We proceed by induction on k, with $n = 2^k$. In the base case, $k = 0$ and $n = 1$, and since $D_2 \cong Z_2$, which is nilpotent (since it is abelian).

Now assume that $D_{2\cdot 2^k}$ is abelian, and consider $D_{2\cdot 2^{k+1}}$. Since $D_{2\cdot 2^{k+1}}/Z(D_{2\cdot 2^{k+1}}) = D_{2\cdot 2^{k+1}}/\langle r^{2^k}\rangle = D_{2\cdot 2^k}$, which is nilpotent, we have that $D_{2\cdot 2^{k+1}}$ is also nilpotent. $\square$

27 Let G be the group of all 3 by 3 upper triangular matrices, with entries in $\mathbb{Z}$, and diagonal entries equal to 1. Prove that the commutator of G is its center.

Proof:

Let $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in Z(G)$, and let $\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in G$. Then,

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

$$\begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+cd+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

$$e + af + b = b + cd + e$$

$$af = cd$$

Since this is true for all $d, f \in \mathbb{Z}$, we have that $a = c = 0$. Hence, a matrix in the center of G is of the form:

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

Now consider elements $A, D \in G$.

$$\begin{aligned}
[A, D] &= ADA^{-1}D^{-1} \\
&= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -d & df-e \\ 0 & 1 & -f \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -(a+d) & (df-e)+af+(ac-b) \\ 0 & 1 & -(c+f) \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & df-e+af+ac-b-ca-cd-fa-fd+e+af+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & af-dc \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

So, since $af - dc \in \mathbb{Z}$, it's clear that $[A, D] \leq Z(G)$. Since $Z(G)$ is a subgroup, it contains all elements generated by elements of the form $[X, Y]$ for $X, Y \in G$. Thus, $G' \leq Z(G)$. Conversely, if $X \in Z(G)$,

then it's of the form above, with top-right entry b. Since we can always pick $a, f, d, c \in \mathbb{Z}$ such that $af - dc = b$, we can construct X as a commutator of elements of G. Therefore, $Z(G) \leq G'$.

Combining these two results, we conclude that $Z(G) = G'$. $\square$

28 Let P be a Sylow p-subgroup of H and $H \leq K$. If P is normal in H and H is normal in K, prove that P is normal in K. Deduce that if $P \in \mathrm{Syl}_p(G)$ then $N_G(P)$ is self-normalizing, i.e., $N_G(N_G(P)) = N_G(P)$.

Proof:

$\underline{P \trianglelefteq K}$:

Let $P \in \mathrm{Syl}_p(H)$. Since $P \trianglelefteq H$, we have $n_p = 1$, and so P is the only subgroup of order p in H. Therefore, P is characteristic in H.

Now, let $k \in K$. Since H is normal, conjugation by k is an automorphism on H. Since P is characteristic in H, we have that $kPk^{-1} = P$. Therefore, $P \trianglelefteq K$. $\square$

$\underline{N_G(P) \text{ is self-normalizing:}}$

Let $P \in \mathrm{Syl}_p(G)$. Recall that $N_G(P)$ is the largest subgroup of G in which P is normal. Since $P \leq N_G(P)$, we have that $P \in \mathrm{Syl}_p(N_G(P))$. Because $N_G(P) \trianglelefteq N_G(N_G(P))$, we have by the above argument, we have that $P \trianglelefteq N_G(N_G(P))$, and so $N_G(N_G(P)) \leq N_G(P)$. But since by definition $N_G(P) \leq N_G(N_G(P))$, we conclude that $N_G(P) = N_G(N_G(P))$, i.e., $N_G(P)$ is self-normalizing. $\square$

29 Prove that if G is a finite group, and each Sylow p-subgroup is normal in G, then G is a direct product of its Sylow subgroups.

Proof:

Let $p_1, \ldots, p_s$ be the distinct primes dividing $|G|$. Let $P_i \in \mathrm{Syl}_{p_i}(G)$ for each i. For any t with $1 \leq t \leq s$, we will show inductively that

$$P_1 P_2 \cdots P_t \cong P_1 \times P_2 \times \cdots \times P_t.$$

Since $P_i \trianglelefteq G$ for each i, we have that the product $P_1 P_2 \cdots P_t$ is in fact a subgroup of G. Let $H := P_1 \times \cdots \times P_{t-1}$ and $K := P_t$. Assume inductively that $H \cong P_1 \cdots P_{t-1}$. Now, $|H| = |P_1||P_2| \cdots |P_{t-1}|$ and $|K| = |P_t|$. Since $\gcd(|H|, |K|) = 1$, we have that $H \cap K = 1$. So, $P_1 P_2 \cdots P_t = HK \cong H \times K = P_1 \times P_2 \times \cdots \times P_t$. This completes the induction. $\square$

30 Classify the abelian groups of order $2^5 \cdot 5^2 \cdot 17^3$.

Proof:

To classify the abelian groups of order $2^5 \cdot 5^2 \cdot 17^3$, we first make the following table:

Order p^β	**Partitions of β**	**Abelian Groups**
2^5	5; 4,1; 3,2; 3,1,1; 2,2,1; 2,1,1,1; 1,1,1,1,1	Z_{32}; $Z_{16} \times Z_2$; $Z_8 \times Z_4$; $Z_8 \times Z_2 \times Z_2$; $Z_4 \times Z_4 \times Z_2$; $Z_4 \times Z_2 \times Z_2 \times Z_2$; $Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$
5^2	2; 1,1	Z_{25}; $Z_5 \times Z_5$
17^3	3; 2,1; 1,1,1	Z_{4913}; $Z_{289} \times Z_{17}$; $Z_{17} \times Z_{17} \times Z_{17}$

Now, the list of abelian groups, up to isomorphism, consists of taking the direct product of one term from each row. So, the list of abelian groups is:

$$Z_{32} \times Z_{25} \times Z_{4913}$$

$$Z_{32} \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_{32} \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_{32} \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_{32} \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_{32} \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_{16} \times Z_2 \times Z_{25} \times Z_{4913}$$

$$Z_{16} \times Z_2 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_{16} \times Z_2 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_{16} \times Z_2 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_{16} \times Z_2 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_{16} \times Z_2 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_8 \times Z_4 \times Z_{25} \times Z_{4913}$$

$$Z_8 \times Z_4 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_8 \times Z_4 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_8 \times Z_4 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_8 \times Z_4 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_8 \times Z_4 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_{25} \times Z_{4913}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_8 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_{25} \times Z_{4913}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_4 \times Z_4 \times Z_2 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{4913}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_4 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{4913}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{289} \times Z_{17}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_{25} \times Z_{17} \times Z_{17} \times Z_{17}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{4913}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{289} \times Z_{17}$$

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_{17} \times Z_{17} \times Z_{17}$$

31 Prove that $(\mathbb{Q}, +)$, the additive group of rational numbers is not cyclic.

Proof:

Assume toward a contradiction that $(\mathbb{Q}, +)$ is cyclic. Then, let $\mathbb{Q} = \langle \frac{a}{b} \rangle$, with $a, b \in \mathbb{Z}$, $b > 0$, and $\gcd(a, b) = 1$. Then, every rational number is an integer multiple of $\mathbb{Q}$, i.e., $\mathbb{Q} = \{n \cdot \frac{a}{b} \mid n \in \mathbb{Z}\}$. Consider $\frac{1}{2b} \in \mathbb{Q}$. Let $r \in \mathbb{Z}$ be such that $r \cdot \frac{a}{b} = \frac{1}{2b}$. Now, we have that $ra = \frac{1}{2}$, which is impossible, since $r, a \in \mathbb{Z}$ and so $ra \in \mathbb{Z}$. Thus we have a contradiction, and so $(\mathbb{Q}, +)$ is not cyclic. □

32 Prove that $\mathrm{Aut}(Z_k)$ is isomorphic to the group $U(k)$ of integers i, with $1 \leq i < k$, which are relatively prime to K, under multiplication modulo k.

Proof:

Let $Z_k = \langle x \rangle$. Recall that any automorphism φ of Z_k is completely determined by $\varphi(x)$, and that $|\varphi(x)| = |x|$. Let $\Phi : \mathrm{Aut}(Z_k) \to U(k)$ be defined by $\Phi : \varphi \mapsto m$, where $\varphi(x) = x^m$. Since x^m must also be a generator of Z_k, it must be true that $m \in U(k)$, and so we have that this mapping is indeed $\mathrm{Aut}(Z_k) \to U(k)$. Φ is surjective because if $\gcd(m, k) = 1$, then $[x \mapsto x^m]$ is an automorphism of $\mathrm{Aut}(Z_k)$. Φ is injective because if $[x \mapsto x^m] = [x \mapsto x^\ell]$, then $m = \ell$. Φ is a homomorphism since for $\varphi : x \mapsto x^m$ and $\psi : x \mapsto x^\ell$, we have that $\varphi \circ \psi : x \mapsto (x^\ell)^m = x^{\ell m}$ and so $\Phi(\varphi \circ \psi) = \ell m = \Phi(\varphi)\Phi(\psi)$. Hence Φ is an isomorphism. Therefore, $\mathrm{Aut}(Z_k) \cong U(k)$. □

33 Give examples of each of the following, with a brief explanation in each case:

(a) A solvable group with trivial center.

(b) An abelian p-group which is isomorphic to one of its proper subgroups and also one of its proper homomorphic images.

(c) An abelian group having no maximal subgroups.

(d) A direct product of nilpotent groups which is not nilpotent.

(e) A semidirect product of abelian groups which is not nilpotent.

(f) A finite nonabelian group in which every proper subgroup is cyclic.

Proof:

(a):

S_3 is solvable. Consider the chain:

$$1 \trianglelefteq \langle (1\ 2\ 3) \rangle \trianglelefteq S_3.$$

Each quotient is abelian. Additionally, the center of S_3 is trivial.

(b):

$Z_p \times Z_p \times \cdots$ is an abelian p group and isomorphic to the proper subgroup $\{1\} \times Z_p \times Z_p \times \cdots$ under the isomorphism $(a_0, a_1, \cdots) \longmapsto (1, a_0, a_1, \cdots)$.

(c):

$(\mathbb{Q}, +)$ is an abelian group with no maximal subgroups (see **Exercise #41** for justification). Additionally, defining multiplication on the set as the zero multiplication, $(\mathbb{Q}, +, \cdot)$ becomes a ring with no maximal ideals because the zero multiplication makes maximal subgroups correspond to maximal ideals.

(d):

Note that $D_{2 \cdot 2^k}$ is nilpotent of class k for all $k \geq 1$. The nilpotency class of a group is greater than or equal to the nilpotency class of its subgroups. Hence, the nilpotency class of a direct product is greater than or equal to the nilpotency class of its terms. Consider the infinite direct product:

$$D_4 \times D_8 \times D_{16} \times D_{32} \times \cdots$$

If this infinite direct product is nilpotent, then its has nilpotency class $\geq k$ for all $k \in \mathbb{N}$, which is clearly not possible. Hence this is a direct product of nilpotent groups which is not nilpotent.

(e):

S_3 is a semidirect product of Z_3 and Z_2, which are abelian. Additionally, S_3 is not nilpotent, because $Z(S_3) = 1$.

(f):

S_3 is finite, nonabelian, and its nontrivial subgroups are isomorphic to Z_2 and Z_3.

34 Each three-cycle in S_n has $\frac{1}{3}n(n-1)(n-2)$ conjugates. Prove this and conclude from it that A_4 is the only subgroup of S_4 of order 12.

Proof:

Since two permutations in S_n are conjugate if and only if they have the same cycle type, the conjugates of a three-cycle are all other three cycles. The number of three cycles in S_n is

$$\binom{n}{3} \cdot 2! = 2\frac{n!}{6(n-3)!} = \frac{1}{3}n(n-1)(n-2).$$

Let $|G| = 12$ with $G \leq S_4$. Since $|S_4 : G| = 2$, we have that $G \trianglelefteq S_4$. So, if G contains a three cycle, then it contains all three cycles. Since $n = 4$, S_4 has $\frac{1}{3} \cdot 4 \cdot 3 \cdot 2 = 8$ three cycles. In this case, G also contains the three (2,2)-cycles, since $(123)(234) = (12)(34)$, $(132)(243) = (13)(24)$, and $(142)(423) = (14)(23)$. So if G contains a three cycle, then $G = A_4$. But, G has a Sylow 3-subgroup, which have two elements of order three, which must be three cycles. So, in fact, $G = A_4$. □

35 Prove that A_5 is a simple group.

Proof:

Any normal subgroup of A_5 must be a union of conjugacy classes. In S_5, conjugacy classes correspond to cycle types. This is not exactly true in A_5. As shown in an earlier exercise, there are two conjugacy classes of 5-cycles, each with 12 5-cycles.

Consider a 3-cycle $\sigma := (1\ 2\ 3)$. There are 20 3-cycles in S_5. Now, the centralizer of σ in A_5 is $\langle(1\ 2\ 3)\rangle$ is $\langle(1\ 2\ 3)\rangle$, and so the index of $C_{A_5}(\langle(1\ 2\ 3)\rangle)$ is $60/3 = 20$. Thus, all 20 3-cycles are conjugate in A_5.

Consider a $(2,2)$-cycle $\sigma = (1\ 2)(3\ 4)$. There are 15 $(2,2)$-cycles in S_5. Now, the centralizer of σ in A_5 is $\langle\{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\}\rangle$, and so the index of $C_{A_5}(\langle(1\ 2)(3\ 4)\rangle)$ is $60/4 = 15$. Thus, all 15 $(2,2)$-cycles are conjugate in A_5.

Now, if A_5 a normal subgroup, then it must be the union of conjugacy classes, which we've shown have order 1, 12, 12, 15, 20. A nontrivial subgroup must have order dividing 60 and not equal to 1 or 60. There is no way to add the numbers 1, 12, 12, 15, 20 (necessarily including the 1), to add up to a number dividing 60. Thus, there are no proper nontrivial normal subgroups of A_5, and so A_5 is simple. □

36 For $n \geq 5$, prove that A_n is the only proper, nontrivial normal subgroup of S_n.

Proof:

Let N be a nontrivial normal subgroup of S_n. Let $\sigma \in N$ be nonidentity. Let i be such that $\sigma(i) \neq i$. Pick $j \in \{1, \ldots, n\}$ such that $j \neq i$ and $j \neq \sigma(i)$. Let $\tau := (i\ j)$. Now,

$$\sigma\tau\sigma^{-1}\tau^{-1} = (\sigma(i)\ \sigma(j))(i\ j).$$

Since $\sigma(i) \notin \{i, j\}$ and $\sigma(i) \neq \sigma(j)$, we have that $(\sigma(i)\ \sigma(j)) \neq (i\ j)$, and thus their product is not the identity.

If $\sigma(j) \neq i$ and $\sigma(j) \neq j$, then $(\sigma(i)\ \sigma(j))(i\ j)$ is a (2,2)-cycle. Otherwise, it is a 3-cycle. Since N is normal it contains either all (2,2)-cycles or all 3-cycles. Since A_n is generated by all 3-cycles and A_n is generated by all (2,2)-cycles, for all $n \geq 5$, we have that $A_n \leq N$. Thus, $N = A_n$ or $N = S_n$. Therefore, A_n is the only proper, nontrivial subgroup of S_n. □

37 Let G be a finite group. Call $x \in G$ a *non-generator* if for each subset $Y \subseteq G$, if $G = \langle Y \cup \{x\} \rangle$ then $G = \langle Y \rangle$. Prove:

(a) The subset $\Phi(G)$ of all non-generators of G form a subgroup of G.

(b) $\Phi(G)$ is the intersection of all maximal subgroups of G.

(c) Conclude from (b) that $\Phi(G)$ is normal.

(d) What is the Frattini subgroup $\Phi(S_n)$? Explain. (Consider the stabilizers of a single letter.)

Proof of (a):

Let, $x, y \in \Phi(G)$. Let $G = \langle Y \cup \{xy^{-1}\} \rangle$. Then,

$$\begin{aligned} G &= \langle Y \cup \{xy^{-1}\} \rangle \\ &\subseteq \langle Y \cup \{x, y\} \rangle \\ &= \langle Y \rangle \\ &\subseteq G. \end{aligned}$$

Hence, $\langle Y \rangle = G$, and so $xy^{-1} \in \Phi(G)$. Thus, $\Phi(G)$ is a subgroup of G. $\square$

Proof of (b):

Let $x \in \Phi(G)$. Let $M \subsetneq G$ be maximal. Assume toward a contradiction that $x \notin M$. Then, $\langle M \cup \{x\} \rangle = G$, and since $x \in \Phi(G)$, we have that $\langle M \rangle = G$, which is a contradiction. Hence, $\Phi(G)$ is contained in every maximal subgroup.

Let x be an element of all maximal subgroups. Let $G = \langle Y \cup \{x\} \rangle$. Assume toward a contradiction that $G \neq \langle Y \rangle$. Then, $\langle Y \rangle \subsetneq \langle Y \cup \{x\} \rangle = G$. If $\langle Y \rangle$ is maximal, then $x \in Y$, which is a contradiction. If $\langle Y \rangle$ is not maximal, then there exists M maximal such that $\langle Y \rangle \subsetneq M \subsetneq G$. Then, $x \in M$, and since $\langle Y \rangle \subset M$, we have that $M = G$, a contradiction. Therefore, $x \in \Phi(G)$.

Hence, $\Phi(G)$ is the intersection of all maximal subgroups of G. $\square$

Proof of (c):

First, observe that the set of all maximal subgroups of G is a union of orbits under the action of $\mathrm{Aut}(G)$ on subgroups of G. This is true because no automorphism can take a maximal subgroup of G to a nonmaximal subgroup of G: if M is maximal and H is not, and $\varphi(H) = M$, then there exists K with $H < K < G$ and $M < \varphi^{-1}(K) < G$, which is a contradiction.

It's clear that if $\mathcal{O}$ is an orbit of the action of $\mathrm{Aut}(G)$ on the subgroups of G, then $\bigcap_{S \in \mathcal{O}} S$ is characteristic in G. This is because the action just permutes the order of elements in $\mathcal{O}$.

Since $\Phi(G)$ is the intersection all maximal subgroups, it is a union of orbits, which is characteristic in G. Hence $\Phi(G)$ is characteristic in G, and thus normal in G. $\square$

Proof of (d):

Since S_{n-1} is a maximal subgroup of S_n and every nonidentity permutation is excluded from some copy of S_{n-1}, we have that $\Phi(S_n) = 1$. $\square$

38 State and prove the Orbit-Stabilizer Theorem.

Orbit-Stabilizer Theorem: If G acts on a set S, then for all $s \in S$:

$$|G| = |\operatorname{Orb}(s)| \cdot |\operatorname{Stab}(s)|.$$

Proof:

Recall that, $|G|/|\operatorname{Stab}(s)|$ is the number of distinct left cosets of $\operatorname{Stab}(s)$ in G. Now, we find a bijection Φ between the left cosets of $|\operatorname{Stab}(s)|$ and $|\operatorname{Orb}(s)|$. Let $\Phi(g\operatorname{Stab}(s)) := g \cdot s$, for $g \in G$ and $s \in S$.

Well-Defined:

Let $g_1\operatorname{Stab}(s) = g_2\operatorname{Stab}(s)$. Then, $g_1^{-1}g_2 \in \operatorname{Stab}(s)$, and so $(g_1^{-1}g_2)(s) = s$. Thus $g_1(s) = g_2(s)$. Hence, the map is well-defined.

Injective:

Let $g_1(s) = g_2(s)$. Then, $(g_2^{-1}g_1)(s) = s$ and so $g_2^{-1}g_1 \in \operatorname{Stab}(s)$. Therefore, $g_2\operatorname{Stab}(s) = g_1\operatorname{Stab}(s)$, and so the map is injective.

Surjective:

Let $t \in \operatorname{Orb}(s)$. Then, there exists $g \in G$ such that $g \cdot s = t$. Now, $\Phi(g\operatorname{Stab}(s)) = g \cdot s = t$. So, Φ is surjective.

Hence, Φ is a bijection between $G/\operatorname{Stab}(s)$ and $\operatorname{Orb}(s)$. Thus, $|G|/|\operatorname{Stab}(s)| = |\operatorname{Orb}(s)|$, and so $|G| = |\operatorname{Stab}(s)||\operatorname{Orb}(s)|$. □

39 Show that if G is a simple abelian group then it is cyclic of prime order.

Proof:

Because G is abelian, any subgroup is normal. Hence, G must have no nontrivial proper subgroups. Let $x \in G$ be non-identity. Then, since $\langle x\rangle \leq G$, we must actually have $\langle x\rangle = G$. So, G is cyclic with generator x.

If G is infinite, then since $\langle x^2\rangle \leq G$, we must have $\langle x^2\rangle = G$. But, $x \notin \langle x^2\rangle$, so this is a contradiction. Therefore, G cannot be infinite.

If G is finite, then assume toward a contradiction that $|G|$ is not prime, so that $|G| = nm$, with $n, m > 1$. Then, $\langle x^n\rangle = G$, but $(x^n)^m = x^{nm} = 1$, and so $m \mid |\langle x^n\rangle|$. Since $m < |G|$, we cannot have that $\langle x^n\rangle = G$. Therefore $|G|$ prime.

So, if G is a simple abelian group, then G is cyclic of prime order. □

40 For the additive group of rational numbers $(\mathbb{Q}, +)$, show that the intersection of any two nontrivial subgroups is nontrivial.

Proof:

Let A, B be nontrivial subgroups of $(\mathbb{Q}, +)$. Let $\frac{a}{b} \in A$ and $\frac{c}{d} \in B$ be nonidentity. Then, $bc\frac{a}{b} = ac \in A$ and $ad\frac{c}{d} = ac \in B$. Hence $ac \in A \cap B$. Since $ac \neq 0$, we have that $A \cap B$ is nontrivial. □

41 Show that the group $(\mathbb{Q}, +)$ of additive rational numbers has no maximal subgroups.

Proof:

Assume toward a contradiction that there exists a maximal subgroup $A \subsetneq \mathbb{Q}$. Since $\mathbb{Q}$ is abelian, $A \trianglelefteq \mathbb{Q}$. By the **Lattice Isomorphism Theorem**, $\mathbb{Q}/A$ has no proper subgroups. So, $\mathbb{Q}/A$ is an abelian simple group. By **Exercise 39**, $\mathbb{Q}/A$ is cyclic of prime order.

$\mathbb{Q}$ is divisible because given any $\frac{m}{n} \in \mathbb{Q}$ and $k \in \mathbb{N}$, we have that $\frac{m}{kn} \cdot k = \frac{m}{n}$.

Since no finite abelian group is divisible (see **Lemma 1** below) and proper quotients of divisible groups are divisible (see **Lemma 2** below), we have that no proper quotient of a divisible group is finite. Hence $\mathbb{Q}/A$ cannot possible have prime (i.e., finite) order. Thus, we have a contradiction, and so $(\mathbb{Q}, +)$ has no maximal subgroups. □

Lemma 1:

Let G be a finite abelian group of order > 1. Let

$$n := \prod_{g \in G} o(g),$$

where $o(g)$ is the order of g. For all $g \in G$, we have that $g^n = 1$. Hence, for all nonidentity $h \in G$, there exists no $x \in G$ such that $x^n = h$. Therefore, G is not divisible.

Lemma 2:

Let G be divisible. Let $N \trianglelefteq G$. Consider G/N. Let $aN \in G/N$ and $k \in \mathbb{N}$. Since G is divisible, there exists $g \in G$ such that $g^k = a$. So, $(gN)^k = g^k N = aN$. Thus, G/N is divisible.

42 The *commutator subgroup* G' of a group G is defined as the subgroup generated by the set

$$\{x^{-1}y^{-1}xy \mid x, y \in G\}.$$

Prove that:

(a) Show that G' is a normal subgroup of G.

(b) Show that G/G' is abelian.

(c) Show that if $\varphi : G \to H$ is a homomorphism into the abelian group H, then there exists a unique homomorphism $\widehat{\varphi} : G/G' \to H$ such that $\widehat{\varphi}(xG') = \varphi(x)$, for each $x \in G$.

Proof of (a):

First we show that for elements of the form $[x, y] := x^{-1}y^{-1}xy$, we have that $g^{-1}[x, y]g \in G'$:

$$\begin{aligned} g^{-1}[x,y]g &= g^{-1}x^{-1}y^{-1}xyg \\ &= g^{-1}x^{-1}gg^{-1}y^{-1}gg^{-1}xgg^{-1}yg \\ &= (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \\ &= [g^{-1}xg,\ g^{-1}yg] \\ &\in G'. \end{aligned}$$

Now, if $h \in G'$, then h is a product of some number of commutators:

$$h = [x_1, y_1] \cdot \cdots \cdot [x_n, y_n],$$

and

$$\begin{aligned} ghg^{-1} &= g[x_1, y_1] \cdot \cdots \cdot [x_n, y_n]g^{-1} \\ &= g[x_1, y_1]g^{-1}g \cdot \cdots \cdot g^{-1}g[x_n, y_n]g^{-1} \\ &\in G'. \ \square \end{aligned}$$

Proof of (b):

Since $G' \trianglelefteq G$, we can consider G/G'. Let $aG', bG' \in G/G'$. Then,

$$\begin{aligned} (aG')(bG') &= abG' \\ &= ab[b, a]G' \\ &= abb^{-1}a^{-1}baG' \\ &= baG' \\ &= (bG')(aG'). \end{aligned}$$

Hence G/G' is abelian. $\square$

Proof of (c):

First we show that $\widehat{\varphi}$ is well defined. If $xG' = yG'$, then $xy^{-1} \in G'$. Now,

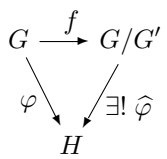
$$\begin{aligned} 1 &= \varphi(1) \\ &= \widehat{\varphi}(G') \\ &= \widehat{\varphi}(xy^{-1}G') \\ &= \varphi(xy^{-1}) \\ &= \varphi(x)\varphi(y)^{-1}. \end{aligned}$$

Thus $\varphi(x) = \varphi(y)$. So, $\widehat{\varphi}(xG') = \varphi(x) = \varphi(y) = \widehat{\varphi}(yG')$.

Next we show that $\widehat{\varphi}$ is a homomorphism:

$$\begin{aligned} \widehat{\varphi}(xG'yG') &= \widehat{\varphi}(xyG') \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) \\ &= \widehat{\varphi}(xG')\widehat{\varphi}(yG'). \end{aligned}$$

We have the following commutative diagram:



The homomorphism is unique because it is well-defined. Any homomorphism $\widehat{\psi}$ defined with $\widehat{\psi}(xG') = \varphi(x)$ has the same value for all $xG' \in G/G'$. $\square$

43 Suppose that G is a group and H is a normal subgroup. Prove that $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Proof:

Let G act on H by conjugation. Since H is normal, this is indeed an action on H. The kernel of this action is

$$\begin{aligned}\{g \in G \mid g \cdot h = h\} &= \{g \in G \mid ghg^{-1}\} \\ &= \{g \in G \mid gh = hg\} \\ &= C_G(H).\end{aligned}$$

Since conjugation by an element on a normal subgroup is an automorphism, we can consider the map $\Phi : G \to \mathrm{Aut}(H)$ by $g \mapsto f_g$, where $f_g(h) := ghg^{-1}$. By the **First Isomorphism Theorem**, we have that $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. □

44 Let G be a group of 385 elements. Prove that the Sylow 11-subgroups are normal, and that any Sylow 7-subgroup lies in the center.

Proof:

Note that $385 = 5 \cdot 7 \cdot 11$. By the Sylow conditions, $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 35$. The only possibility is that $n_{11} = 1$, and hence the single Sylow 11-subgroup is normal. Similarly, we have that $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 55$, and so $n_7 = 1$. Hence the single Sylow 7-subgroup is normal. Let $P \in \mathrm{Syl}_7(G)$. By **Exercise 43**, $G/C_G(P) \cong$ [a subgroup of $\mathrm{Aut}(P)$]. Since $\mathrm{Aut}(P)$ has order 6, it's subgroups have possible orders $\{1, 2, 3, 6\}$, and so $C_G(P)$ has order in $\{385/1, 385/2, 385/3, 385/6\}$. Of those possibilities, only $385/1 = 385$ is an integer, and so $|C_G(P)| = 385$. Thus, we conclude that $C_G(P) = G$, and so P lies in the center of G. □

45 Describe all groups of 44 elements, up to isomorphism.

Proof:

By the **Fundamental Theorem of Finitely Generated Abelian Groups**, the abelian groups of order 44 are Z_{44} and $Z_2 \times Z_{22}$. Let $P \in Syl_{11}(G)$ and let $Q \in \mathrm{Syl}_2(G)$. Observe that $|Q| = 4$. By the Sylow conditions, we have that $P \trianglelefteq G$. So, we consider semidirect products $P \rtimes_\varphi Q$ where $\varphi : Q \to \mathrm{Aut}(P)$ is nontrivial.

Since $|Q| = 4$, we have two possibilities for Q: either $Q \cong Z_4$ or $Q \cong Z_2 \times Z_2$. We consider these cases separately.

In the case where $Q \cong Z_4$, it's clear that Q has two elements of order 2, one element of order 4, and the identity. Since $P \cong Z_{11} = \langle x \rangle$, we have that $\mathrm{Aut}(P) \cong Z_{10}$, which has one element of order two (the map $x \mapsto x^{-1}$) and no elements of order four. So, the only map $Q \to \mathrm{Aut}(P)$ maps the generator q of Q to the inverse map on P. We call this map φ_1.

In the case where $Q \cong Z_2 \times Z_2$, it's clear that Q has three elements of order 2 and the identity. An nontrivial automorphism from Q to $\mathrm{Aut}(P)$ must map two of the three elements of order two to the inverse map, and the third to the identity map. However, all three of these homomorphisms differ (over composition) by an automorphism on Q. Hence, they all yield the same semidirect product. We call this map φ_2.

So, the two nonabelian semidirect products are:

$$G_1 := \langle (h,k) \mid h \in Z_{11}, k \in Z_4,\ (h,k)(h',k') = (h[\varphi_1(k)](h'), kk') \rangle$$

$$G_2 := \langle (h,k) \mid h \in Z_{11}, k \in V_4,\ (h,k)(h',k') = (h[\varphi_2(k)](h'), kk') \rangle$$

To see that these two groups are non-isomorphic, find the number of elements of order two in each group.

In G_1, let $(h,k)^2 = 1$. Then,

$$(h\varphi_1(k)(h), k^2) = 1 = (1,1).$$

Let $\langle y \rangle = Q$. If $k = y$ or y^3, then $k^2 \neq 1$. If $k = 1$ or $k = y^2$, then $(h\varphi_1(k)(h), k^2) = (h^2, 1)$, and so (h,k) has order two if $h \neq 1$ and h has order two in $Z_{11} = \langle x \rangle$. There are no such h. Thus the only possibility for an element of order two is $(1, y^2)$. So, G_1 has one element of order two.

In G_2, let $(h,k)^2 = 1$. Then,

$$(h\varphi_2(k)(h), k^2) = 1 = (1,1).$$

In the two cases where $\varphi_2(k)$ is the identity map, we need that $h^2 = 1$ and $k^2 = 1$, with h, k both not 1. Well, $k^2 = 1$ for all elements of Q, and as above h has no elements of order two, so this gives rise to one element of order two. In the two cases where $\varphi_2(k)$ is the inverse map, we can pick any element h. So, here we have 22 elements of order two. Thus, G_2 has 23 elements of order 2.

Observing the action of an element of order two on an element of order 22 in G_2 and that we have the proper number of elements of order two, we conjecture that $G_2 \cong D_{44}$. □

46 Suppose that $|G| = 105$. If G has a normal Sylow 3-subgroup, prove that it must lie in the center of G.

Proof:

Let $P \in \mathrm{Syl}_3(G)$ be normal. By **Exercise 43**, $G/C_G(P) \cong$ [a subgroup of $\mathrm{Aut}(P)$]. Since $\mathrm{Aut}(P)$ has order 2, we have that $C_G(P)$ has order 105 or 105/2. Since 105/2 is not an integer, $|C_G(P)| = 105$, and so $C_G(P) = G$. Thus, $P \in Z(G)$. □

47 Let G and H be the cyclic groups of order n and k respectively. Prove that the number of homomorphisms from G to H is the sum of all $\varphi(d)$, where d runs over all common divisors of n and k, and φ denotes the Euler φ function.

Proof:

Let $G = \langle x \rangle$ and $H = \langle y \rangle$. If $f \in \mathrm{Hom}(G,H)$, then f is completely determined by the image of x. We must have that $|f(x)| \mid k$ and $|f(x)| \mid n$. Therefore, the number of possible homomorphisms is the sum over all $d \mid \gcd(n,k)$ of the number of elements of order d in H.

An element $h \in H$ has order d if and only if $h^d = 1$ and $h^m \neq 1$ for $1 \leq m < d$. So, an element $h \in H$ has order d if and only if for some q, $h = y^{qb}$, where $b := k/d$, and $\gcd(d, |h|) = 1$. The elements h with $h = y^{qb}$ are the subgroup $\langle y^b \rangle$. Of these d elements, the number of these with order relatively prime to d is $\varphi(d)$. Hence, for each order d dividing both n and k, there are $\varphi(d)$ elements of H to which we can send the generator x, which completely determines any homomorphism form G to H. So,

$$|\mathrm{Hom}(G,H)| = \sum_{d \mid \gcd(n,k)} \varphi(d). \ \square$$

1.3 Rings

48 Let R be the ring of all n by n matrices with integer entries. Prove that the matrix $A \in R$ is invertible if and only if its determinant is ± 1.

Proof:

Use the **Cofactor Formula for the Inverse of a Matrix** found on pg. 440 of *Dummit & Foote*. A consequence of this theorem is that for $A \in R$ is a unit in R (i.e., invertible) if and only if its determinant is a unit in $\mathbb{Z}$. Since the only units in $\mathbb{Z}$ are ± 1, the theorem follows. $\square$

49 Using Zorn's Lemma, prove that each non-zero commutative ring with an identity has maximal ideals.

Proof:

Let R be a non-zero commutative ring. We will show that any proper ideal is contained in a maximal ideal. Since the zero ideal is a proper ideal in a non-zero ring, we will conclude that in any non-zero ring, maximal ideals exist.

Let Σ be the set of proper ideals of R which contain the zero ideal. Since every ideal contains the zero ideal, Σ is simply the set of proper ideals of R. Clearly, Σ is nonempty, since $(0) \in \Sigma$. Let Σ be partially ordered by upward inclusion, i.e., $I_1 \leq I_2$ if and only if $I_1 \subseteq I_2$.

Let $\mathscr{C}$ be a chain of Σ. Let $\mathscr{I} := \bigcup_{I \in \mathscr{C}} I$. We will show that $\mathscr{I}$ is an upper bound of the chain $\mathscr{C}$.

First, we need to show that $\mathscr{I} \in \Sigma$, i.e., that $\mathscr{I}$ is a proper ideal of R. To see this:

(1) Let $a, b \in \mathscr{I}$. Then, since $\mathscr{C}$ is a chain and $\mathscr{I}$ is the union of the sets in the chain, there exists $I \in \mathscr{C}$ such that $a, b \in I$. Since I is an ideal, it is a subring of R and thus closed under addition and multiplication. So, $a + b \in R$ and $ab \in R$. Since $I \subseteq \mathscr{I}$ by the definition of $\mathscr{I}$, we have that $a + b \in \mathscr{I}$ and $ab \in \mathscr{I}$. Thus, $\mathscr{I}$ is a subring of R.

(2) Let $a \in \mathscr{I}$ and $r \in R$. Then, there exists $I \in \mathscr{C}$ such that $a \in I$. Since I is an ideal, we have that $ra \in \mathscr{I}$. Since $I \subseteq \mathscr{I}$ by the definition of $\mathscr{I}$, we have that $ra \in \mathscr{I}$. Thus, $\mathscr{I}$ is an ideal of R.

(3) Assume toward a contradiction that $\mathscr{I}$ is not a proper ideal of R, i.e., $\mathscr{I} = R$. Then, $1 \in \mathscr{I}$. So, there exists some $I \in \mathscr{C}$ such that $1 \in I$, and so $I = R$. This is a contradiction, since $R \notin \mathscr{C}$. Hence, $\mathscr{I}$ is a proper ideal of R.

(4) Since every ideal contains the zero ideal, $(0) \subseteq \mathscr{I}$.

So, $\mathscr{I} \in \Sigma$.

Now, it's clear that $\mathscr{I}$ is an upper bound of the chain $\mathscr{C}$, since it contains (by inclusion) each element of the chain $\mathscr{C}$. By Zorn's Lemma, there exist a maximal element (by inclusion) $\mathscr{M} \in \Sigma$. To see that $\mathscr{M}$ is a maximal ideal of R, observe that if not, then there is an ideal T such that $\mathscr{M} \subsetneq T \subsetneq R$, and since $(0) \subsetneq \mathscr{M}$ and T proper, this contradicts the maximality of $\mathscr{M}$. Hence $\mathscr{M}$ is a maximal ideal of R, and so R contains a maximal ideal. $\square$

50 Using Zorn's Lemma, prove that in each non-zero commutative ring with identity, minimal prime ideals exist. **Proof:**

Let R be a non-zero commutative ring. Let Σ be the set of all prime ideals. Let Σ be ordered by downward inclusion, so that for $I_1, I_2 \in \Sigma$, we have that $I_1 \leq I_2$ if and only if $I_1 \supseteq I_2$.

By the previous exercise, R has a maximal ideal. Since all maximal ideals are prime ideals, R has a prime ideal. Therefore, $\Sigma \neq \emptyset$. Let $\mathscr{C}$ be a chain of Σ. Let $\mathscr{P} = \bigcap_{I \in \mathscr{C}} I$.

Now we show that $\mathscr{P}$ is an upper bound of the chain $\mathscr{C}$. First we show that $\mathscr{P} \in \Sigma$, i.e., that $\mathscr{P}$ is a prime ideal of R:

(1) Let $a, b \in \mathscr{P}$. Then, $a, b \in I$ for all $I \in \mathscr{C}$. Since I is an ideal, $a + b \in I$ and $ab \in I$ for all $I \in \mathscr{C}$. Thus, $a + b \in \mathscr{P}$ and $ab \in \mathscr{P}$. Therefore, PP is a subring of R.

(2) Let $a \in \mathscr{P}$ and $r \in R$. Then, $a \in I$ for all $I \in \mathscr{C}$. Since I is an ideal, $ra \in I$ for all $I \in \mathscr{C}$. Thus, $ra \in \mathscr{P}$ and so $\mathscr{P}$ is an ideal.

(3) Let $ab \in \mathscr{P}$. Then, $ab \in I$ for all $I \in \mathscr{C}$. Assume toward a contradiction that there exists $I_1 \in \mathscr{C}$ with $a \notin I_1$ and $b \notin I_2$. Without loss of generality, $I_1 \subseteq I_2$ and so $b \notin I_1$. This contradicts the fact that I_1 is prime. So, either $a \in I$ for all $I \in \mathscr{C}$ or $b \in I$ for all $I \in CC$. Thus either $a \in \mathscr{P}$ or $b \in PP$. Therefore, $\mathscr{P}$ is a prime ideal.

So, $\mathscr{P} \in \Sigma$. Additionally, $\mathscr{P}$ is an upper bound for this chain because it is a subset of every element of the chain.

By Zorn's Lemma, there exists a maximal element $\mathscr{M}$ of Σ. To see that $\mathscr{M}$ is a minimal prime ideal of R, assume toward a contradiction that it isn't. Then, there exists a prime ideal Q with $(0) \subsetneqq Q \subsetneqq \mathscr{M}$. In this case, we have that $Q \in \mathscr{C}$ and $\mathscr{M} < Q$, which contradicts the maximality of $\mathscr{M}$ in Σ. Therefore, $\mathscr{M}$ is a minimal prime ideal of R, and so minimal prime ideals exist. □

51 Consider $A = \mathbb{R}^{\mathbb{N}}$, the ring of all real valued sequences, under pointwise operations. Prove:

(a) For each $n \in \mathbb{N}$, $M_n = \{f(n) = 0\}$ is a maximal ideal of A;

(b) There exist maximal ideals besides the M_n ($n \in \mathbb{N}$). Use Zorn's Lemma.

Proof of (a):

First we show that M_n is an ideal in A:

(a) Let $f, g \in M_n$, then $(f + g)(n) = 0$ and $(fg)(n) = 0$, and so $f + g \in M_n$ and $fg \in M_n$. Thus, M_n is a subring of A.

(b) Let $r \in A$. Then, $(rf)(n) = 0$, and so $rf \in M_n$. Thus, M_n is an ideal of A.

Assume toward a contradiction that M_n is not maximal in A. Then, there exists an ideal S of A such that $M_n \subsetneqq S \subsetneqq A$. Then, there exists $f \in S$ with $f(n) \neq 0$. Say $f(n) = s$. Then, for all $a := (a_1, a_2, \ldots) \in A$, we have that $\ell := (a_1, \ldots, a_{n-1}, 0, a_{n+1}, \ldots) \in S$ and $k := (0, \ldots, a_n/s, \ldots) \in S$, and so $\ell + kf = a \in S$. Thus, $S = A$, which is a contradiction. So, M_n is maximal in A. □

Proof of (b):

We know that every proper ideal is contained in a maximal ideal. So, if we find a proper ideal I that is not contained in any M_n, then the maximal ideal that contains also does not contains it any of the M_n and so we will know that there does exist a maximal ideal besides the M_n.

Let I be the set of real valued sequences that have only a finite number of non-zero terms.

(1) If $i_1, i_2 \in I$, then clearly $i_1 + i_2 \in I$.

(2) If $i_1, i_2 \in I$, then clearly $i_1 \cdot i_2 \in I$.

(3) In fact, if $i_1 \in I$ and $r \in A$, then $i_1 r \in I$ and $r i_1 \in I$.

Therefore, I is an ideal which is obviously proper. It is not contained in any of the M_n because the sequences with a non-zero term in the n^{th} slot and zeros everywhere else are in I, but not in M_n. Thus, the maximal ideal that contains this proper ideal is not any of the M_n. □

52 Suppose that A is a commutative ring with identity. Suppose that $a \in A$ is not nilpotent. Prove that there is a prime ideal that fails to contain a. Use this to show that the set of all nilpotent elements of A is the intersection of all prime ideals of A.

Proof:

Let $a \in A$ be not nilpotent. Let Σ be the set of ideals not containing a^m, for all $m \in \mathbb{N}$. Σ contains the zero ideal, due to the fact that a is not nilpotent, and therefore $\Sigma \neq \emptyset$. Let Σ be partially ordered under inclusion. Let $\mathscr{C}$ be a chain of Σ. Let $\mathscr{I} := \bigcup_{I \in \mathscr{C}} I$. We show that $\mathscr{I}$ is an upper bound of $\mathscr{C}$:

(1) Let $a, b \in \mathscr{I}$. Then, since $\mathscr{C}$ is a chain and $\mathscr{I}$ is the union of the sets in the chain, there exists $I \in \mathscr{C}$ such that $a, b \in I$. Since I is an ideal, it is a subring of R and thus closed under addition and multiplication. So, $a + b \in R$ and $ab \in R$. Since $I \subseteq \mathscr{I}$ by the definition of $\mathscr{I}$, we have that $a + b \in \mathscr{I}$ and $ab \in \mathscr{I}$. Thus, $\mathscr{I}$ is a subring of R.

(2) Let $a \in \mathscr{I}$ and $r \in R$. Then, there exists $I \in \mathscr{C}$ such that $a \in I$. Since I is an ideal, we have that $ra \in \mathscr{I}$. Since $I \subseteq \mathscr{I}$ by the definition of $\mathscr{I}$, we have that $ra \in \mathscr{I}$. Thus, $\mathscr{I}$ is an ideal of R.

(3) Additionally, $a^m \neq \mathscr{I}$ for all $m \in \mathbb{N}$, since then we would have $a^m \in I$ for some $I \in \mathscr{C}$, which is a contradiction.

So, $\mathscr{I}$ is an upper bound of $\mathscr{C}$. Therefore, by Zorn's Lemma, there exists a maximal element $\mathscr{P}$. This maximal element is an ideal that does not contain a^m for all $m \in \mathbb{N}$. However, note that this does <u>not</u> imply that $\mathscr{P}$ is a maximal ideal of R.

Now, we show that $\mathscr{P}$ is a prime ideal. Let $x, y \in R$ such that $xy \in \mathscr{P}$. Assume toward a contradiction that $x \notin \mathscr{P}$ and $y \notin \mathscr{P}$. Then, $(\mathscr{P}, x) \supsetneq \mathscr{P}$ and $(\mathscr{P}, y) \supsetneq \mathscr{P}$. So, by the maximality of $\mathscr{P}$, we have that $a^m \in (\mathscr{P}, x)$ and $a^n \in (\mathscr{P}, y)$ for some $m, n \in \mathbb{N}$. Thus, we can write $a^m = p_1 + r_1 x$ and $a^n = p_2 + r_2 y$ for some $p_1, p_2 \in \mathscr{P}$ and $r_1, r_2 \in R$. Now,

$$a^{m+n} = p_1 p_2 + p_1 r_2 y + p_2 r_1 x + r_2 r_2 xy.$$

The right hand side of that equation lies in $\mathscr{P}$ (since $p_1, p_2, xy \in \mathscr{P}$, and $\mathscr{P}$ is an ideal), and the left side is not in $\mathscr{P}$ by construction. This is a contradiction. Therefore, $\mathscr{P}$ is a prime ideal that does not contain a. □

To show that the set of nilpotent elements is the intersection of all prime ideals of A, we need to show inclusion in both directions. The above proof shows that any element that is in all prime ideals is nilpotent. Now, let $a \in R$ be nilpotent, with m such that $a^m = 0$. Let $\mathscr{P}$ be a prime ideal. Note that $0 \in \mathscr{P}$. Since $a^{m-1} \cdot a = 0 \in \mathscr{P}$, we have that either $a^{m-1} \in \mathscr{P}$ or $a \in \mathscr{P}$. Assume toward a contradiction that $a \notin \mathscr{P}$, then $a^{m-1} \in \mathscr{P}$, and we can repeat this process to conclude that actually $a \in \mathscr{P}$. Hence, every nilpotent element is in every prime ideal. □

53 Let F be a field, and $A = F[[x]]$ denote the ring of formal power series in one variable. Prove the following:

(a) The units of A are precisely the power series whose constant term is nonzero.

(b) Suppose that $k \geq 1$ is an integer. Let I_k denote the set of all power series $\sum_{n=0}^{\infty} a_n x^n$ for which $a_0, \ldots, a_{k-1}$ are all zero. Each I_k is an ideal of A.

(c) If J is a nonzero proper ideal of A, then $J = I_m$, for some $m \geq 1$.

Proof of (a):

Let $f(x) = \sum a_n x^n \in F[[x]]$ with constant term nonzero. Since F is a field, we define $b_0 := a_0^{-1}$. For each b_n for $n > 0$, we want that

$$0 = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k},$$

and so we set $b_n := -\left(\sum_{k=1}^{n} a_k b_{n-k}\right) a_0^{-1}$.

Now, by construction $\left(\sum a_n\right)\left(\sum b_n\right) = \sum c_n$ where $c_0 = 1$ and $c_n = 0$ for all $n > 0$. Thus $\sum b_n$ is the inverse of $f(x)$ and so $f(x)$ is a unit in $F[[x]]$.

Conversely, let $f(x)$ be a unit of A. Then, there exists $g(x) \in A$ such that $f(x)g(x) = \mathbf{1}$. Note that the constant term of $f(x)g(x)$ is $a_0 b_0$, and so we have that $a_0 b_0 = 1$. Thus, a_0 is a unit of F and so a_0 is nonzero. $\square$

Proof of (b):

Let k be fixed. Let $f(x), g(x) \in I_k$. Then, the first k coefficients of $f(x) + g(x)$ are $0 + 0 = 0$ and so $f(x) + g(x) \in I_k$. Also, the $(m+1)^{\text{th}}$ coefficient of $f(x)g(x)$ for $0 \leq m \leq k-1$ is

$$\sum_{i=0}^{m} f_i g_{m-i} = \sum_{i=0}^{m} 0 \cdot 0 = 0.$$

Thus, $f(x)g(x) \in I_k$. Hence we conclude that I_k is a subring of A. Now let $r(x) \in A$. Then, for $0 \leq m \leq k-1$, the $(m+1)^{\text{th}}$ coefficient of $r(x)f(x)$ is

$$\sum_{i=0}^{m} r_i f_{m-i} = \sum_{i=0}^{m} r_i \cdot 0 = \sum_{i=0}^{m} 0 = 0.$$

Therefore, I_k is an ideal of A. $\square$

Proof of (c):

Let J be a nonzero proper ideal. If $J \neq I_m$ for all m, then J has an element $f(x)$ with nonzero constant term. By **part (a)**, this is an unit in $F[[x]]$, and so $J = R$, and J is no longer proper. Hence, $J = I_m$ for some $m \in \mathbb{N}$. $\square$

54 Prove the Division Algorithm for the ring $\mathbb{Z}[i]$ of Gaussian integers.

Proof:

Let $\alpha := a + bi$ and $\beta := c + di$, such that $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$.

Let N be the usual complex norm: $N(x + yi) := x^2 + y^2$.

Consider that $\dfrac{\alpha}{\beta} = r + si$, where $r = \dfrac{ac + bd}{c^2 + d^2}$ and $s = \dfrac{bc - ad}{c^2 + d^2}$.

Pick p to be the closest integer to r, and pick q to be the closest integer to s. This gives us the property that $|r - p| \leq \dfrac{1}{2}$ and $|s - q| \leq \dfrac{1}{2}$.

Let $\theta := (r-p)+(s-q)i$. Clearly, θ is the difference between $\dfrac{\alpha}{\beta}$ and $p+qi$. That is, $\theta = \dfrac{\alpha}{\beta} - (p+qi)$. Now let $\gamma := \theta\beta = \alpha - (p + qi)\beta$. Rearranging: $\alpha = (p + qi)\beta + \gamma$.

It remains to show that $N(\gamma) < N(\beta)$. In fact, $N(\gamma) = N(\theta\beta) = N(\theta)N(\beta)$.

Since $N(\theta) < \dfrac{1}{4} + \dfrac{1}{4} = \dfrac{1}{2}$, we have that $N(\gamma) \leq \dfrac{1}{2}N(\beta)$. $\square$

55 Let D be an integer which is not a square in $\mathbb{Z}$. Consider the subring $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$; (do not prove it is a subring.) Define $N(a + b\sqrt{D}) = a^2 - Db^2$. Assume that $N(xy) = N(x)N(y)$, for all $x, y \in \mathbb{Z}[\sqrt{D}]$. Prove that

(a) $a + b\sqrt{D}$ is a unit of $\mathbb{Z}[\sqrt{D}]$ if and only if $N(a + b\sqrt{D}) = \pm 1$.

(b) If $D < -1$, prove that the units of $\mathbb{Z}[\sqrt{D}]$ are precisely ± 1.

Proof of (a):

($\Rightarrow$)

Assume $A := a + b\sqrt{D}$ has an inverse $B := c + f\sqrt{D}$. Now, $(a + b\sqrt{D})(c + f\sqrt{D}) = 1$. So, $N(AB) = N(A)N(B) = N(1) = 1$. Since $N(A), N(B) \in \mathbb{Z}$, we have that $N(A) = \pm 1$. $\square$

($\Leftarrow$)

Let $N(a + b\sqrt{D}) = 1$. Then, $a^2 - Db^2 = 1$. Observe that:

$$(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 = 1,$$

and so $a + b\sqrt{D}$ is a unit.

Let $N(a + b\sqrt{D}) = -1$. Then, $a^2 - Db^2 = -1$. Observe that:

$$(a + b\sqrt{D})(-a + b\sqrt{D}) = -(a^2 - Db^2) = -(-1) = 1,$$

and so $a + b\sqrt{D}$ is a unit. $\square$

Proof of (b):

Let $D < -1$. Let $a + b\sqrt{D}$ be a unit of $\mathbb{Z}[\sqrt{D}]$. Then, $N(a + b\sqrt{D}) = a^2 - Db^2 = \pm 1$. Since $a+b\sqrt{D}$ is not zero, either $a^2 \geq 1$ and $b^2 \geq 1$. If $b^2 \geq 1$, then $-Db^2 > 1$, which is a contradiction. Hence $b = 0$, and so $a = \pm 1$. Hence $a + b\sqrt{D} = \pm 1$. □

56 A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Prove:

(a) Every boolean ring has characteristic 2 and is commutative.

(b) Assume R is a boolean ring. Prove that every prime ideal is maximal.

Proof of (a):

Since $x^2 = x$, we have that $x^2 - x = 0$ for all $x \in R$. Note that $-1 \in R$ because it is the additive inverse of 1. Substituting $x = -1$, we see that $0 = (-1)^2 - (-1) = 1 + 1$. So, $1 + 1 = 0$, and thus R has characteristic 0.

Also, $(x + y) = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Thus, $0 = xy + yx$ and hence $xy = -yx$. But, because R has characteristic 2, we have that $-x = x$ for all $x \in R$ and so $xy = yx$. Thus, R is commutative. □

Proof of (b):

Let R be an abelian ring. Let P be a prime ideal. Then, we have that R/P is an integral domain.

Let $x \notin P$. Then, $P \neq x + P \in R/P$. Now, $x + P = x^2 + P$, and so $x^2 - x = x(x - 1) \in P$. Since $x \notin P$, we have that $x - 1 \in P$. Thus, $x \in 1 + P$.

So, R/P has two cosets, P and $1 + P$, and therefore, $R/P \cong \mathbb{F}_2$. Since R/P is a field, we have that P is a maximal ideal. Therefore, in a boolean ring, every prime ideal is a maximal ideal. (Recall that in any commutative ring with 1, any maximal ideal is a prime ideal.) □

57 A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Assume the preceding exercise. Use the Chinese Remainder Theorem to prove that every finite boolean ring has 2^n elements, for a suitable non-negative integer n.

Proof v1: (Not using CRT)

Assume toward a contradiction that $|R| = m$, where $p \mid m$ for some prime $p \neq 2$. Since $(R, +)$ is an additive group, by **Cauchy's Theorem**, there exists $x \neq 0$ such that $|x| = p$ in $(R, +)$. So, in R, we have that $px = 0$. Since p is odd, we can set n such that $p = 2n + 1$. now, $0 = px = (2n + 1)x = 2(nx) + x$. Since boolean rings have characteristic 2 by the previous exercise, $2r = 0$ for all $r \in R$. So, $0 = x$, which is a contradiction. Thus, $|R|$ is a power of two. □

Proof v2: (Using CRT)

Let $\{A_i\}$ be the set of maximal ideals of R. By the previous exercise, each A_i is a prime ideal. By another previous exercise, the intersection of all prime ideals is the set of nilpotent elements of R. However, boolean rings have no nonzero nilpotent elements, because if $x \neq 0$, then $x^i = x \neq 0$ for all $i \in \mathbb{N}$. So, $\cap(A_i) = \{0\}$. Since each pair A_i, A_j is comaximal, we apply the **Chinese Remainder Theorem** to see that $\cap(A_i) = \prod(A_i)$, and $R/(\prod(A_I)) \cong R/A_1 \times \cdots \times R_/A_k$. So,

$$R/A_1 \times \cdots \times R/A_k \cong R/(\prod(A_i)) = R/(\bigcap(A_i)) \cong R.$$

But as in the previous exercise, for any prime ideal P, we have that $R/P \cong Z_2$, as rings. So,

$$R \cong Z_2 \times \cdots \times Z_2.$$

Thus, $|R|$ is a power of two. $\square$

58 Suppose that A is a nonzero commutative ring with identity. Let $n(A)$ denote the set of nilpotent elements of A; you may assume here that it is an ideal. Prove the equivalence of the following three statements:

(a) Every nonunit of A is nilpotent.

(b) $A/n(A)$ is a field.

(c) A has exactly one prime ideal.

Proof:

(a) $\Longrightarrow$ (c):

Assume every nonunit of A is nilpotent. First we show that $n(A)$ is a prime ideal. Let $ab \in n(A)$. Then, $(ab)^m = 0$ for $m \in \mathbb{N}$. By commutativity $a^m b^m = 0$. Assume that $a \notin n(A)$, so that a is not nilpotent. Then, a is a unit, and so a^{-1} exists. Thus, $(a^{-1})^m a^m b^m = 0$, and so $b^m = 0$, and hence $b \in n(A)$. Hence, $n(A)$ is a prime ideal.

Now, since $n(A)$ is the intersection of all prime ideals by a previous exercise, its clear that it is the only prime ideal. If there were another prime ideal, it would contain a non-nilpotent element, which would be a unit, and then the ideal would be all of R, and hence not prime. $\square$

(c) $\Longrightarrow$ (b):

Assume A has exactly one prime ideal. Since $n(A)$ is a proper ideal, there exists a maximal ideal M that contains $n(A)$. Since all maximal ideals are prime, we have that $M = n(A)$. So, $n(A)$ is a maximal ideal. Therefore, $A/n(A)$ is a field. $\square$

(b) $\Longrightarrow$ (a):

Let $x \notin n(A)$. Then, by assumption, there exists $y \notin n(A)$ such that $(x+n(A))(y+n(A)) = 1 + n(A)$. Now, $xy \in 1 + n(A)$, and so $xy = 1 + n$, for some $n \in n(A)$. Since it will work out better, we actually write $xy = 1 - n$, for $n \in n(A)$. Since n is nilpotent, let m be the smallest positive integer such that $n^m = 0$. Now, note that

$$1 = 1 - n^m = (1 - n)(1 + n + n^2 + \cdots + n^{m-1}).$$

Hence, $1-n = xy$ is a unit in A. Therefore, there exists $z \in A$ such that $(xy)z = z(xy) = 1$. Since A is commutative, we rearrange this to:

$$x(yz) = (yz)x = 1$$

and hence x is a unit of A. Therefore, every non-nilpotent element of A is a unit, which is the contrapositive of the statement to be proved. $\square$

59 Prove the Chinese Remainder Theorem: if A is a commutative ring with identity, and I and J are comaximal ideals of A, then $IJ = I \cap J$, and the homomorphism $\varphi : A \to A/I \times A/J$ defined by $\varphi(a) = (a + I, a + J)$ is surjective.

Proof:

Consider the map $\varphi : A \to A/I \times A/J$ defined by $\varphi(a) = (a + I, a + J)$. This map is a ring homomorphism because φ is just the natural projection of A into A/I and A/J for the two components. The kernel of φ consists of all the elements $a \in A$ that are in I and J, i.e., $I \cap J$. To complete the proof, it remains to show that when I and J are comaximal, it follows that φ is surjective and $I \cap J = IJ$. Since $I + J = A$, there are elements $x \in I$ and $y \in J$ such that $x + y = 1$. This equation shows that $\varphi(x) = (0, 1)$ and $\varphi(y) = (1, 0)$ since, for example, x is an element of I and $x = 1 - y \in 1 + J$. If now $(a_1 \mod I, a_2 \mod J)$ is an arbitrary element in $A/I \times A/J$, then the element $a_2x + a_1y$ maps to this element since:

$$\begin{aligned}\varphi(a_2x + a_1y) &= \varphi(a_2)\varphi(x) + \varphi(a_1)\varphi(y)\\ &= (a_2 \bmod I, a_2 \bmod J)(0, 1) + (a_1 \bmod I, a_1 \bmod J)(1, 0)\\ &= (0, a_2 \bmod J) + (a_1 \bmod I, 0)\\ &= (a_1 \bmod I, a_2 \bmod J).\end{aligned}$$

This shows that φ is indeed surjective. Finally, the ideal IJ is always contained in $I \cap J$ (since an element in IJ is a finite sum of elements of the form ij, which each of those terms in $I \cap J$ by the ideal property, and so the sum is in $I \cap J$). If I and J are comaximal and x and y are as above, then for any $c \in I \cap J$,

$$c = c1 = c(x + y) = cx + cy \in IJ.$$

This establishes the reverse inclusion $A \cap B \subseteq AB$, and completes the proof. □

Note that the actual Chinese Remainder Theorem is on an arbitrary number k of ideals. This is the $k = 2$ case. To prove the general case, start with the above, and the induction follows easily.

60 Let D be an integral domain. Prove that the ring $D[T]$ of polynomials over D in one indeterminate is a principal ideal domain if and only if D is a field.

Proof:

($\Longrightarrow$):

Let $D[T]$ be a principal ideal domain for some integral domain D. The ideal (T) is a nonzero prime ideal in $D[T]$ because $D[T]/(T)$ is isomorphic to the integral domain D. Since every nonzero prime ideal in a Principal Ideal Domain is maximal, we have that (T) is a maximal ideal. Therefore, the $D[T]/(T)$ is a field, and hence D is a field. □

($\Longleftarrow$):

Let D be a field. Consider the ring $D[T]$ of polynomials over D in one indeterminate. We will show that $D[T]$ is actually Euclidean Domain. Since every Euclidean Domain is a Principal Ideal Domain, the theorem will then follow.

Let $f(T) \in D[T]$. Let $\deg(f(T))$ be the degree of the polynomial $f(T)$. This function is a norm. So, it remains to show that given $f(T), g(T) \in D[T]$, there exist unique $q(T), r(T) \in D[T]$ such that $f(T) = q(T)g(T) + r(T)$, with $r(T) = 0$ or $\deg(r(T)) < \deg(g(T))$.

If $f(T) = 0$, then we can set $q(T) = r(T) = 0$. If $\deg(f(T)) < \deg(g(T))$, then we can set $q(T) \equiv 0$ and $r(T) = f(T)$. So, from now on, we assume that $f(T) \neq 0$ and

$\deg(f(T)) \geq \deg(g(T))$. We proceed by induction on $n = \deg(f(T))$. If $\deg(f(T)) = 0$, then $f(T)$ is a constant and since D is a field, the result follows.

Now, assume the theorem holds for all $f(T)$ with $\deg(f(T)) < n$, and now let $\deg(f(T)) = n$. Let $\deg(g(T)) =: k$. Since we're assuming that $\deg(g(T)) \leq \deg(f(T))$, we have that $k \leq n$. Let $f(T) = a_0 + a_1T + \cdots + a_nT^n$ and let $g(T) = b_0 + b_1T + \cdots + b_kT^k$. Since D is a field, b_k has an inverse, and so we can define $h(T) := f(T) - a_nb_k^{-1}x^{n-k}g(T)$. This $h(T)$ has degree $\leq n-1$. So, by the induction hypothesis, there exists $q'(T)$ and $r'(T)$ such that $h(T) = q'(T)g(T) + r'(T)$, with $r'(T) = 0$ or $\deg(r'(T)) < \deg(g(T))$. Now, defining $q(T) := q'(T) + a_nb_k^{-1}x^{n-k}$ and $r(T) := r'(T)$, we have that:

$$\begin{aligned} q(T)g(T) + r(T) &= (q'(T) + a_nb_k^{-1}x^{n-k})g(T) + r(T) \\ &= q'(T)g(T) + a_nb_k^{-1}x^{n-k}g(T) + r(T) \\ &= (q'(T)g(T) + r(T)) + a_nb_k^{-1}x^{n-k}g(T) \\ &= h(T) + (f(T) - h(T)) \\ &= f(T). \end{aligned}$$

So, since $D[T]$ is a Euclidean Domain, it is also a Principal Ideal Domain. □

61 Let A be a commutative ring with 1. Suppose that I and J are ideals of A. Prove that:

(a) Prove that $IJ \subseteq I \cap J$, and given an example where equality does not hold.

(b) Suppose that A is the (ring) direct product of two fields. Show that $IJ = I \cap J$, for any two ideals I and J of A.

Proof of (a):

Let $\sum_r i_rj_r \in IJ$. Since I is a (two-sided) ideal, $i_rj_r \in I$ for all r. Since J is a (two-sided) ideal, $i_rj_r \in J$ for all r. Therefore, $i_rj_r \in I \cap J$ for all r, and by the additive closure of ideals, we have that $\sum_r i_rj_r \in I \cap J$. Therefore, $IJ \subseteq I \cap J$. □

For an example where equality does not hold, let $A := \mathbb{Z}$, $I := 4\mathbb{Z}$ and $J := 6\mathbb{Z}$. Now, $IJ = 24\mathbb{Z}$ and $I \cap J = 12\mathbb{Z}$. Since $24\mathbb{Z} \subsetneq 12\mathbb{Z}$, this containment is proper.

Proof of (b):

Let $A := F_1 \times F_2$, where F_1 and F_2 are fields. We already showed one containment in **part (a)**.

Let I and J be ideals of A and let $(x, y) \in I \cap J$. Since F_1 is a field x^{-1} exists. Since F_2 is a field, y^{-1} exists. Since $I \cap J$ is an ideal, we have that

$$(x^{-1}, 1)(x, y) = (1, y) \in I \cap J \subseteq I,$$

and

$$(1, y^{-1})(x, y) = (x, 1) \in I \cap J \subseteq J.$$

Therefore,

$$IJ \ni (1, y)(x, 1) = (x, y).$$

So, we have shown that $I \cap J \subseteq IJ$, and therefore $IJ = I \cap J$ in this case. □

62 Suppose that D is an integral domain. A polynomial $f(x)$ over D is *primitive* if the greatest common divisor of its coefficients is 1.

Prove the following form of Gauss' Lemma: If D is a unique factorization domain, then the product of any two primitive polynomials over D is primative.

Proof:

Let $c(f)$ denote the gcd of all coefficients of $f(x)$. Let f, g be primative, i.e., $c(f) = c(g) = 1$. Assume toward a contradiction that $c(fg) = d > 1$. Let p be a prime factor of d. Then, p divides every coefficient in fg. Since $c(f) = 1$, there exists a minimal n such that p does not divide the coefficient of x^n in f. Since $c(g) = 1$, there exists a minimal m such that p does not divide the coefficient of x^m in g.

Consider the coefficient of x^{m+n} in fg:

$$a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_nb_m + \cdots + a_{m+n-1}b_1 + a_{m+n}b_0.$$

Note that $p \nmid a_nb_m$, since p is prime. But, p divides all of the terms because $p \mid a_i$ for all $i < n$ and $p \mid b_i$ for all $i < m$. Thus, p does not divide the coefficient of x^{m+n} in fg, and so $c(fg) \neq p$. This is a contradiction. Therefore, $c(fg) = 1$. □

63 Let A be an integral domain, and P be a prime ideal of A. Define A_P to be the subset of the quotient field K of A, consisting of all fractions whose denominator is not in P. Prove that

(a) A_P is a subring of K;

(b) A_P has exactly one maximal ideal; identify it.

Proof of (a):

Let $A_P = \{a/b \mid a \in A,\ b \in A \setminus P\}$. Let $a/b,\ c/d \in A_P$. Then,

$$\frac{a}{b} + \frac{c}{d} = \frac{ac + bd}{bd}.$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd}.$$

Since P is prime and $b, d \notin P$, we have that $bd \notin P$. Therefore, A_P is closed under addition and multiplication. Because A_P is a subset of K, we conclude that A_P is a subring of K. □

Proof of (b):

Let $A^P := \{a/b \mid a \in P,\ b \in A \setminus P\}$. We will show that A^P is a maximal ideal of A_P by showing that A_P/A^P is a field.

First we show that A^P is an ideal of A_P. Let $a/b,\ c/d \in A^P$. Then: $a/b + c/d = (ad + bc)/(bd)$, and $ad, bc \in P$ (by the ideal property), and $bd \notin P$ since P prime. Therefore A^P is closed under addition. If $a/b \in A^P$ and $c/d \in A_P$, then $(a/b) \cdot (c/d) = (ac)/(bd)$, with $ac \in P$ and $bd \notin P$ as above. Hence, A^P is an ideal of A_P.

Let $x = \dfrac{a}{b} \in A_P \setminus A^P$. Then, $x^{-1} = \dfrac{b}{a} \in A_P$, and therefore the coset $x + A^P$ has inverse $x^{-1} + A^P$. Since every nonzero coset has an inverse, we must have that A_P/A^P is a field. Therefore, A^P is a maximal ideal. □

64 (a) Define *Euclidean Domain* and *Principal Ideal Domain*.

(b) Prove that any Euclidean Domain is a Principal Ideal Domain.

Part (a):

Let R be an integral domain. A *norm* on R is a function $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(0) = 0$. R is said to be a *Euclidean Domain* if there exists a norm N on R such that for any two elements a and b of R with $b \neq 0$, there exist elements q and r in R with

$$a = qb + r, \quad \text{with } r = 0 \text{ or } N(r) < N(b).$$

An ideal generated by a single element is called a *principal ideal*. A *Principal Ideal Domain* is an integral domain in which every ideal is principal.

Proof of (b):

Let R be a Euclidean domain with norm N. Let I be an ideal of R. If I is the zero ideal, then the theorem holds. So, let $0 \neq d \in I$ be any element of minimum norm (which exists by the Well Ordering of $\mathbb{Z}$). Clearly, $(d) \subseteq I$. To show the reverse inclusion, let $a \in I$. Using the Division Algorithm that comes with a Euclidean Domain, we can write $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Then, $r = a - qd$, and since both $a, qd \in I$ we have that $r \in I$. By the minimality of the norm of d, we must have that $r = 0$, and so $a = qd \in (d)$. Therefore $I = (d)$, and so I is principal. Since I was an arbitrary ideal of R, it follows that R is a Principal Ideal Domain. □

65 Convince that the polynomial rings $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ have the same field of fractions, but the power series rings $\mathbb{Z}[[X]]$ and $\mathbb{Q}[[X]]$ do not.

Proof:

Let $\mathrm{FOF}(R)$ denote the field of fractions of the ring R.

Since $\mathbb{Z} \subseteq \mathbb{Q}$ and consequently $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$, it is clear that $\mathrm{FOF}(\mathbb{Z}[X]) \subseteq \mathrm{FOF}(\mathbb{Q}[X])$. However, letting $f(X)/g(X) \in \mathrm{FOF}(\mathbb{Q}[X])$, it's clear that we can multiply by some integer on the top and bottom to clear denominators of both f and g simultaneously, making $f(X)/g(X)$ into a fraction on integer polynomials. Therefore, $\mathrm{FOF}(\mathbb{Q}[X]) \subseteq \mathrm{FOF}(\mathbb{Z}[X])$, and so the two are equal.

As above, it's clear that $\mathrm{FOF}(\mathbb{Z}[[X]]) \subseteq \mathrm{FOF}(\mathbb{Q}[[X]])$. To see that the reverse inclusion is not true, consider the power series expansion of e^X:

$$\alpha := e^X = \sum_{n \geq 0} \frac{1}{n!} X^n.$$

Assume toward a contradiction that $\alpha \in \mathrm{FOF}(\mathbb{Z}[[X]])$. Then, there exist nonzero $u, v \in \mathbb{Z}[[X]]$ such that $u\alpha = v$. Write $u = \sum a_i x^i$ and $v = \sum b_j x^j$. Then, by comparing coefficients, we have

$$b_n = \sum_{i+j=n} \frac{a_i}{j!},$$

for all $n \geq 1$. Hence,

$$\frac{a_0}{n} = (n-1)! b_n - \sum_{\substack{i+j=n \\ i \neq 0}} \frac{a_i (n-1)!}{j!}.$$

Since the term on the right is an integer for all $n \in \mathbb{N}$, we have that a_0 is divisible by all integers. Therefore $a_0 = 0$, and hence $b_0 = 0$. Repeating this process, we get that $a_i = b_i = 0$ for all $i \in \mathbb{N}$, which is a contradiction. Therefore, $\alpha \notin \mathrm{FOF}(\mathbb{Z}[[X]])$. □

66 Consider the polynomial X^2+1 over the field $\mathbb{Z}/7\mathbb{Z}$. Prove that $E = (\mathbb{Z}/7\mathbb{Z})[X]/(X^2+1)$ is a field of 49 elements.

Proof:

Let $f(X) := X^2+1$. Observe that

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(2) &= 5 \\ f(3) &= 3 \\ f(4) &= 3 \\ f(5) &= 5 \\ f(6) &= 2 \end{aligned}$$

Therefore, $f(X)$ has no roots in $\mathbb{Z}/7\mathbb{Z}$, and so $f(X)$ is irreducible in $(\mathbb{Z}/7\mathbb{Z})[X]$. Hence, (X^2+1) is a maximal ideal of $(\mathbb{Z}/7\mathbb{Z})[X]$. Thus, $(\mathbb{Z}/7\mathbb{Z})[X]/(X^2+1)$ is a field.

Now, since $\mathbb{Z}/7\mathbb{Z}$ is a field, observe that every element of E can be written as $a+bX+(X^2+1)$, since for any $p(x) \in (\mathbb{Z}/7\mathbb{Z})[X]$, there exists $q(X)$ and $r(X)$ with $\deg(r) < 2$ such that

$$p(X) = q(X)(X^2+1) + r(X),$$

and so $p(X) \equiv r(X) \bmod (X^2+1)$. Since each element $a+bX+(X^2+1)$ for $a, b \in \mathbb{Z}/7\mathbb{Z}$ is distinct, we have that E contains exactly $7 \cdot 7 = 49$ elements. □

67 Let n be a natural number; prove that the polynomial

$$\Phi_n(X) := \frac{X^n-1}{X-1}$$

is irreducible over the ring $\mathbb{Z}$ precisely when n is prime.

Proof:

Note that

$$\frac{X^n-1}{X-1} = X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1.$$

Note also that

$$\Phi_n(X+1) = \frac{(X+1)^n - 1}{X} = X^{n-1} + nX^{n-2} + \cdots + \frac{n(n-1)}{2}X + n.$$

If n is prime, then by **Eisenstein's Criterion**, we have that Φ_n is irreducible.

If $n = ab$ for $a, b > 1$, then we can factor $X^{ab-1} + \cdots + X + 1$ as:

$$\begin{aligned} X^{n-1} + \cdots + X + 1 &= X^{n-a}\left(X^{a-1} + \cdots + 1\right) + X^{n-2a}\left(X^{a-1} + \cdots + 1\right) + \cdots + (X^{a-1} + \cdots + 1) \\ &= (X^{a-1} + \cdots + 1)(X^{n-a} + X^{n-2a} + \cdots + 1). \end{aligned}$$

Hence in this case $\Phi_n(X)$ is reducible.

Therefore, $\Phi_n(X)$ is irreducible if and only if n is prime. □

68 Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

Proof:

Consider $x^2 + y^2 - 1 \in \mathbb{Q}[x, y] = \mathbb{Q}[y][x]$. Since $\mathbb{Q}[y]$ is a Euclidean Domain, it is a Unique Factorization Domain. Thus, since $y - 1 \in \mathbb{Q}[y]$ is irreducible, we have that $(y - 1)$ is a prime ideal of $\mathbb{Q}[y]$. Now, we see that $x^2 + (y^2 - 1) = x^2 + (y - 1)(y + 1)$ is irreducible by Eisenstein's Criterion, because $y^2 - 1 \in (y - 1)$, but $y^2 - 1 \notin (y - 1)^2$. □

69 Give examples of the following, and justify your choices:

(a) A unique factorization domain which is not a principal ideal domain.

(b) A local integral domain with a *nonzero* prime ideal that is not maximal.

(c) An integral domain in which the uniqueness provision of "unique factorization" fails.

Proof of (a):

The integer polynomial ring $\mathbb{Z}[x]$ is not a principal ideal domain because the ideal generated by $(2, x)$ is not principal: Assume toward a contradiction that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Then, since $2 \in (a(x))$, there must be some $p(x)$ such that $2 = p(x)a(x)$. Thus, $p(x)$ and $a(x)$ are both constants. We cannot have that $a(x) = \pm 1$ since then $(a(x)) = \mathbb{Z}[x]$. Therefore, $a(x) = \pm 2$. But, this implies that $x \in (a(x)) = (2) = (-2)$, and so $x = 2q(x)$ for some polynomial $q(x) \in \mathbb{Z}[x]$, which is a contradiction. Therefore, $(2, x)$ is not principal in $\mathbb{Z}[x]$.

However, recall that if R is a Unique Factorization Domain, then so is $R[x]$. Therefore, $\mathbb{Z}[x]$ is a Unique Factorization Domain which is not a Principal Ideal Domain. □

Proof of (b):

A local integral domain R by definition has a unique maximal (two-sided) ideal. Consider the ring of formal power series in two variables $\mathbb{Q}[[x, y]]$. It's clear that (x, y) is an ideal which is maximal, since any term not in (x, y) is a constant, which is a unit. Now, the ideal (x) is prime because if $f(x)g(x) \in (x)$, then neither $f(x), g(x)$ have any terms with y, and both cannot be constant, and so either $f(x) \in (x)$ or $g(x) \in (x)$. Thus, (x) is a nonzero prime ideal which is not maximal (because it is properly contained in (x, y)) in a local integral domain. □

Proof of (c):

Consider the Quadratic Integer Ring $\mathbb{Z}[\sqrt{-5}]$. Note that in this ring:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Since $2 \nmid 1 \pm \sqrt{-5}$, we have that this is two nonidentical factorizations of 6 in the ring $\mathbb{Z}[\sqrt{-5}]$, even though $\mathbb{Z}[\sqrt{-5}]$ is clearly an integral domain. □

1.4 Modules

70 Suppose that F is a field and G is a multiplicative subgroup of $F \setminus \{0\}$. Prove that G is cyclic.

Proof:

Note that G must be abelian because it is a multiplicative subgroup of a field. By the **Fundamental Theorem of Finitely Generated Abelian Groups**, we have that

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

where $n_k \mid n_{k-1} \mid \cdots \mid n_1$.

Since n_k divides the order of each of these cyclic groups, we have that each factor contains n_k elements of order dividing n_k. If $k > 1$, then there would be more than n_k elements of order dividing n_k, and so there would be more than n_k roots of the polynomial $x^{n_k} - 1 \in F[x]$, which is a contradiction. Hence, $k = 1$, and so G is cyclic. □

71 Suppose that F is a field and $q(x) := a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ is an irreducible polynomial in $F[x]$. Prove that $E = F[x]/(q(x))$ is a field which is an n dimensional vector space in F.

Proof:

Since $q(x)$ is irreducible, we have that $(q(x))$ is a maximal ideal, and so $F[x]/(q(x))$ is a field. To see that it is an n dimensional vector space over F, we show that $\mathscr{B} := \{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\}$ is a basis of $F[x]/(q(x))$.

Firstly, let $a(x) \in F[x]$. By the Euclidean Algorithm (since $F[x]$ is a Euclidean Domain), there exists $c(x), d(x) \in F[x]$ such that $a(x) = q(x)c(x) + d(x)$, with $\deg(d(x)) < n$. Therefore, $a(x) + (q(x)) \in \text{Span}(\mathscr{B})$.

Now, assume toward a contradiction that there exists $b_0, b_1, \ldots, b_{n-1}$ not all zero such that

$$b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1} = 0.$$

Then,

$$b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + (q(x)) = 0 + (q(x)),$$

and so $q(x) \mid b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1}$.

But, this implies that $\deg(q(x)) \mid n - 1$, which is a contradiction. Therefore the set $\mathscr{B}$ is linearly independent.

Since it spans E and is linearly independent, we conclude that $\mathscr{B}$ is a basis for E. □

72 Let R be a ring with identity and M be an R-module. An element $x \in M$ is called a *torsion element* if $rx = 0$ for some nonzero $r \in R$. Let $T(M)$ denote the subset of all torsion elements of M.

(a) If R is an integral domain, show that $T(M)$ is a submodule of M.

(b) Give an example to show that $T(M)$ in general is not a submodule of M.

Proof of (a):

Let R be an integral domain. Let $x, y \in T(M)$. So, there exists $a, b \in R$ such that $ax = by = 0$. Since R is commutative, we see that

$$ab(x + ry) = (ab)x + (ab)ry = b(ax) + ra(by) = 0.$$

Note that $ab \neq 0$ because R is an integral domain. Thus, $x + ry \in T(M)$, and so we have that $T(M)$ is a submodule. □

Proof of (b):

Consider the ring $\mathbb{Z}/12\mathbb{Z} =: M$ as a module over itself. Now,

$$\begin{aligned} 2 \cdot 6 = 0 &\implies 2 \in T(M) \\ 3 \cdot 4 = 0 &\implies 3 \in T(M) \\ 4 \cdot 3 = 0 &\implies 4 \in T(M) \\ 6 \cdot 2 = 0 &\implies 6 \in T(M) \\ 8 \cdot 3 = 0 &\implies 8 \in T(M) \\ 9 \cdot 4 = 0 &\implies 9 \in T(M) \\ 10 \cdot 6 = 0 &\implies 10 \in T(M) \end{aligned}$$

If $T(M)$ is a module, then $2 + 3 = 5 \in T(M)$, but this is clearly false. Therefore, in general, $T(M)$ is not a submodule of M. $\square$

73 Suppose that A is a commutative ring with identity, and I is an ideal of A.

(a) For each positive integer n, prove that

$$A^n/IA^n \cong A/I \times \cdots A/I.$$

(b) Use (a) to prove that if $A^m \cong A^n$, where m and n are positive integers, then $m = n$. (You may use the corresponding fact for fields.)

Proof of (a):

First we show that $IA^n = (IA)^n$. Let $x \in IA^n$. Then, we can write

$$x = \sum_j i_j(a_{j,1}, \cdots, a_{j,n}).$$

Now,

$$\begin{aligned} x &= \sum_j i_j(a_{j,1}, \cdots, a_{j,n}) \\ &= \sum_j (i_j a_{j,1}, \cdots, i_j a_{j,n}) \\ &= \left(\sum_j i_j a_{j,1}, \cdots, \sum_j i_j a_{j,n} \right) \in (IA)^n. \end{aligned}$$

To see the reverse inclusion, let $x \in (IA)^n$ be written as

$$x = \left(\sum_j i_j a_{j,1}, \cdots, \sum_j i_j a_{j,n} \right).$$

Then, letting $e_i := (0, \cdots, 0, 1, 0, \cdots, 0)$ be the sequence with a 1 in the i^{th} spot and 0 elsewhere,

$$\begin{aligned}
x &= \left(\sum_j i_{j,1} a_{j,1}, \ \cdots, \ \sum_j i_{n,j} a_{j,n} \right) \\
&= \sum_i \left[\left(\sum_j i_{j,1} a_{j,1}, \cdots, \sum_j i_{j,n} a_{j,n} \right) e_i \right] \\
&= \sum_i \left[\sum_j \left[(i_{j,1} a_{j,1}, \cdots, i_{j,n} a_{j,n}) \, e_i \right] \right] \\
&= \sum_i \left[\sum_j \left[i_{j,i} ((a_{j,1}, \cdots a_{j,n}) e_i) \right] \right] \\
&= \sum_i \left[i_{i,i} \sum_j \left[(a_{j,1}, \cdots a_{j,n}) e_i \right] \right] \in IA^n.
\end{aligned}$$

Hence $IA^n = (IA)^n$. Therefore, it's clear that

$$A^n/(IA^n) \cong A^n/(IA)^n.$$

Next we show that

$$A^n/(IA)^n = (A \times \cdots \times A)/(IA \times \cdots \times IA) \cong A/IA \times \cdots \times A/IA.$$

Consider the map

$$\varphi : A^n/(IA)^n \longrightarrow A/IA \times \cdots \times A/IA$$

defined by

$$(a_1, \cdots, a_n) + (IA)^n \longmapsto (a_1 + IA, \ \cdots, \ a_n + IA).$$

First we show that φ is well-defined. Let $(x_1, \cdots, x_n), (y_1, \cdots, y_n) \in A^n/(IA)^n$ such that

$$(x_1, \cdots, x_n) + (IA)^n = (y_1, \cdots, y_n) + (IA)^n.$$

To show well-definedness, we have to show that $x_i + IA = y_i + IA$, i.e., $x_i - y_i \in IA$, for all i. By assumption, $(x_1 - y_1, \cdots, x_n - y_n) \in (IA)^n$, we have that $x_i - y_i \in IA$ for all i, and thus φ is well-defined.

To see that φ is injective, we reverse the process. If $x_i + IA = y_i + IA$ for all i, then $(x_1, \cdots, x_n) - (y_1, \cdots, y_n) \in (IA)^n$, and so $(x_1, \cdots, x_n) + (IA)^n = (y_1, \cdots, y_n) + (IA)^n$.

It is clear that φ is surjective.

Lastly, we check the homomorphism property of φ.

$$\begin{aligned}
\varphi\left(((a_1, \cdots, a_n) + (IA)^n)((b_1, \cdots, b_n) + (IA)^n)\right) &= \varphi\left((a_1, \cdots, a_n)(b_1, \cdots, b_n) + (IA)^n\right) \\
&= \varphi\left((a_1 b_1, \cdots, a_n b_n) + (IA)^n\right) \\
&= (a_1 b_1 + IA, \cdots, a_n b_n + IA) \\
&= ((a_1 + IA)(b_1 + IA), \cdots, (a_n + IA)(b_n + IA)) \\
&= (a_1 + IA, \cdots, a_n + IA)(b_1 + IA, \cdots, b_n + IA) \\
&= \varphi\left((a_1, \cdots, a_n) + (IA)^n\right) \varphi\left((b_1, \cdots, b_n) + (IA)^n\right).
\end{aligned}$$

So, we have shown that φ is an isomorphism. Now, we conclude that

$$A^n/IA^n \cong A^n/(IA)^n \cong A/IA \times \cdots A/IA.$$

Lastly, an element $x \in IA$ can be written as

$$\sum_j i_j a_j = \sum_j i'_j \in I$$

where $i'_j = i_j a_j \in I$ by the ideal property. Since it's obvious that $I \subseteq IA$, we conclude that $I = AI$, and this completes the last step of the proof:

$$A^n/IA^n \cong A^n/(IA)^n \cong A/IA \times \cdots A/IA \cong A/I \times \cdots A/I. \ \square$$

Proof of (b):

Let I be a maximal ideal of A, which exists because every ring has at least one maximal ideal. Now, A/I is a field. Assume that $A^m \cong A^n$. By **part (a)**:

$$\underbrace{A/I \times \cdots \times A/I}_{n \text{ times}} \cong A^n/IA^n \cong A^m/IA^m \cong \underbrace{A/I \times \cdots \times A/I}_{m \text{ times}}.$$

By the corresponding fact for fields applied to the above conclusions that

$$(A/I)^n \cong (A/I)^m,$$

we conclude that $n = m$. $\square$

74 Prove that $\mathbb{Q}$, the additive group of the rationals, is not a free abelian group.

Proof:

We think of $\mathbb{Q}$ not as an abelian group, but as a $\mathbb{Z}$-module. Since $\mathbb{Q}$ is a field, it's also an integral domain, and we can calculate its rank. The rank of an integral domain is the maximum size of any linearly independent set of elements of $\mathbb{Q}$. Let $a/b,\ c/d \in \mathbb{Q}$ be nonzero. Now,

$$(bc)(a/b) + (-ad)(cd) = (ac) + (-ac) = 0.$$

And since $bc, -ad \in \mathbb{Z}$ are not both zero, we have that the set $\{a/b,\ c/d\}$ is not linearly independent. Therefore the rank of $\mathbb{Q}$ is 1.

So, if $\mathbb{Q}$ is a free abelian group (i.e., a free $\mathbb{Z}$-module), then it follows that $\mathbb{Q}$ has a basis consisting of one element, i.e.,

$$\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle = \left\{ n \cdot \frac{a}{b} \mid n \in \mathbb{Z} \right\}$$

for some nonzero $a/b \in \mathbb{Q}$. However, it's clear that

$$\frac{a}{2b} \in \mathbb{Q} \setminus \left\langle \frac{a}{b} \right\rangle,$$

and therefore $\mathbb{Q}$ cannot be a free abelian group. $\square$

75 Suppose that G is an abelian group, generated by x_1, x_2, x_3, x_4, and subject to the relations:

$$4x_1 - 2x_2 - 2x_3 = 0, \quad 8x_1 - 12x_3 + 20x_4 = 0, \quad 6x_1 + 4x_2 - 16x_4 = 0.$$

Write G as a direct product of cyclic groups.

Proof:

Write as a matrix:

$$\begin{pmatrix} 4 & -2 & -2 & 0 \\ 8 & 0 & -12 & 20 \\ 6 & 4 & 0 & -16 \end{pmatrix}.$$

Now, row reduce over $\mathbb{Z}$:

$$\begin{pmatrix} 4 & -2 & -2 & 0 \\ 8 & 0 & -12 & 20 \\ 6 & 4 & 0 & -16 \end{pmatrix} \xrightarrow{C_1 \longleftrightarrow C_2} \begin{pmatrix} -2 & 4 & -2 & 0 \\ 0 & 8 & -12 & 20 \\ 4 & 6 & 0 & -16 \end{pmatrix} \xrightarrow{-C_1 \longrightarrow C_1}$$

$$\begin{pmatrix} 2 & 4 & -2 & 0 \\ 0 & 8 & -12 & 20 \\ -4 & 6 & 0 & -16 \end{pmatrix} \xrightarrow{2R_1+R_3 \longrightarrow R_3} \begin{pmatrix} 2 & 4 & -2 & 0 \\ 0 & 8 & -12 & 20 \\ 0 & 14 & -4 & -16 \end{pmatrix} \xrightarrow{-2C_1+C_2 \longrightarrow C_2}$$

$$\begin{pmatrix} 2 & 0 & -2 & 0 \\ 0 & 8 & -12 & 20 \\ 0 & 14 & -4 & -16 \end{pmatrix} \xrightarrow{-C_1+C_3 \longrightarrow C_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 8 & -12 & 20 \\ 0 & 14 & -4 & -16 \end{pmatrix} \xrightarrow{-2R_2+R_3 \longrightarrow R_3}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 8 & -12 & 20 \\ 0 & -2 & 20 & -56 \end{pmatrix} \xrightarrow{R_2 \longrightarrow R_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2 & 20 & -56 \\ 0 & 8 & -12 & 20 \end{pmatrix} \xrightarrow{-C_2 \longrightarrow C_2}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 20 & -56 \\ 0 & -8 & -12 & 20 \end{pmatrix} \xrightarrow{4R_2+R_3 \longrightarrow R_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 20 & -56 \\ 0 & 0 & 68 & -214 \end{pmatrix} \xrightarrow{-10C_2+C_3 \longrightarrow C_3}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & -56 \\ 0 & 0 & 68 & -214 \end{pmatrix} \xrightarrow{28C_2+C_4 \longrightarrow C_4} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 68 & -214 \end{pmatrix} \xrightarrow{3C_3+C_4 \longrightarrow C_4}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 68 & 0 \end{pmatrix}.$$

So, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{68}$. $\square$

76 Let R be a commutative ring with identity. If F is a free R-module of rank $n < \infty$, show that $\mathrm{Hom}_R(F, M) \cong M^n$ for each R-module M.

Proof:

Since F is free of finite rank n, F has a basis $A := \{a_1, \cdots, a_n\}$, and $F \cong F(A)$. In particular, F has the same universal property as $F(A)$, and so $F \cong Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$. Recall the following theorems:

(1) $\mathrm{Hom}_R(R, M) \cong M$. (see proof below)

(2) $\mathrm{Hom}_R(A \times B, M) \cong \mathrm{Hom}_R(A, M) \times \mathrm{Hom}_R(B, M)$. (see proof below)

Therefore,

$$\mathrm{Hom}_R(F, M) \cong \mathrm{Hom}_R(R^n, M) \cong [\mathrm{Hom}_R(R, M)]^n \cong M^n. \ \square$$

Proof of (1):

Let $\varphi \in \mathrm{Hom}_R(R, M)$. Since R is a module over itself, and the ring R has a 1, we have that for all $r \in R$:

$$\varphi(r) = \varphi(r \cdot 1_R) = r\varphi(1_R).$$

Therefore, φ is completely determined by $\varphi(1_R)$.

So, define a map

$$\Phi : \mathrm{Hom}_R(R, M) \to M$$

defined by

$$\Phi : \varphi \mapsto \varphi(1_R).$$

We will show that Φ is an isomorphism.

First, note that if $\varphi, \psi \in \mathrm{Hom}_R(R, M)$, then

$$\begin{aligned}\Phi(\varphi + r\psi) &= (\varphi + r\psi)(1_R) \\ &= \varphi(1_R) + (r\psi)(1_R) \\ &= \varphi(1_R) + r\psi(1_R) \\ &= \Phi(\varphi) + r\Phi(\psi).\end{aligned}$$

Hence, Φ is a homomorphism.

Let $\varphi \neq \psi$. Then, there exists $r \in R$ such that $\varphi(r) \neq \psi(r)$. Therefore, $r\varphi(1_R) \neq r\psi(1_R)$, and thus $\varphi(1_R) \neq \psi(1_R)$. Hence, $\Phi(\varphi) \neq \Phi(\psi)$, and so Φ is injective.

Lastly, let $m \in M$. Define a homomorphism $\varphi \in \mathrm{Hom}_R(R, M)$ by $\varphi(1_R) := m$. As above, this determines the entire map, which is an R-module homomorphism by the Universal Property of Module Homomorphisms. Hence Φ is surjective.

So, we have shown that Φ is an isomorphism, and therefore

$$\mathrm{Hom}_R(R, M) \cong M. \ \square$$

Proof of (2):

Let A, B, M be R-modules. Consider the map

$$\Phi : \mathrm{Hom}_R(A, M) \times \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A \times B, M)$$

defined by

$$\Phi : (\varphi, \psi) \mapsto [\alpha : (a, b) \to \varphi(a) + \psi(b)].$$

First, let $\varphi \in \mathrm{Hom}_R(A, M)$ and $\psi \in \mathrm{Hom}_R(B, M)$. We check that $\Phi(\varphi, \psi)$ is indeed a homomorphism in $\mathrm{Hom}_R(A \times B, M)$. Well, it's clear that $\Phi(\varphi, \psi)$ maps elements in $A \times B$ to elements in M, and so it remains to check the homomorphism property:

$$\begin{aligned}\Phi(\varphi, \psi)((a_1, b_1) + r(a_2, b_2)) &= \Phi(\varphi, \psi)(a_1 + ra_2, b_1 + rb_2) \\ &= \varphi(a_1 + ra_2) + \psi(b_1 + rb_2) \\ &= \varphi(a_1) + r\varphi(a_2) + \psi(b_1) + r\psi(b_2) \\ &= (\varphi(a_1) + \psi(b_1)) + r(\varphi(a_2) + r\psi(b_2)) \\ &= \Phi(\varphi, \psi)(a_1, b_1) + r\Phi(\varphi, \psi)(a_2, b_2).\end{aligned}$$

Thus, $\Phi(\varphi, \psi) \in \mathrm{Hom}_R(A \times B, M)$.

Now, we show that Φ is a homomorphism.

$$\begin{aligned}\Phi((\varphi_1,\psi_1)+r(\varphi_2,\psi_2))(a,b) &= \Phi(\varphi_1+r\varphi_2,\psi_1+r\psi_2)(a,b)\\ &= (\varphi_1+r\varphi_2)(a)+(\psi_1+r\psi_2)(b)\\ &= \varphi_1(a)+\psi_1(b)+r(\varphi_2(a)+\psi_2(b))\\ &= \Phi(\varphi_1,\psi_1)(a,b)+r\Phi(\varphi_2,\psi_2)(a,b)\\ &= (\Phi(\varphi_1,\psi_1)+r\Phi(\varphi_2,\psi_2))(a,b).\end{aligned}$$

Therefore, Φ is a homomorphism.

To see that Φ is surjective, pick $\alpha \in \mathrm{Hom}(A\times B, M)$. Since

$$\alpha(a,b) = \alpha((a,0)+(0,b)) = \alpha(a,0)+\alpha(0,b),$$

we can define φ,ψ by

$$\begin{aligned}\varphi(a) &:= \alpha(a,0),\\ \psi(b) &:= \alpha(0,b).\end{aligned}$$

When defined like this, φ,ψ are homomorphisms because α is a homomorphism. Now, $\Phi(\varphi,\psi) = \alpha$, and so Φ is surjective.

To see that Φ is injective, let $(\varphi,\psi) \in \operatorname{Ker}\Phi$. Then, $0 = \Phi(\varphi,\psi)(a,0) = \varphi(a)$ for all $a \in A$ and so $\varphi \equiv 0$. Similarly, $\psi \equiv 0$. Therefore, $\operatorname{Ker}\Phi$ is trivial and so Φ is injective.

Hence, Φ is an isomorphism, and thus

$$\mathrm{Hom}_R(A\times B, M) \cong \mathrm{Hom}_R(A,M)\times \mathrm{Hom}_R(B,M). \ \square$$

77 Let V be a vector space over the field F. Suppose that U_1 and U_2 are finite dimensional subspaces of V. Prove that $\dim(U_1)+\dim(U_2) = \dim(U_1\cap U_2)+\dim(U_1+U_2)$.

Proof:

Let U_1 have basis $\{a_1,\ldots,a_n\}$ and let U_2 have basis $\{b_1,\ldots,b_m\}$. U_1+U_2 is defined to be the vector space spanned by $U_1\cup U_2$. Therefore, U_1+U_2 is spanned by $\{a_1,\ldots,a_n,b_1,\ldots,b_m\}$ (though this may not be a linearly independent set).

Let $U_1\cap U_2$ have basis $\{c_1,\ldots,c_k\}$. Now, since $U_1\cap U_2$ is a subspace of U_1, we can use the replacement theorem to see that $\{c_1,\ldots,c_k,a_{k+1},\ldots,a_n\}$ is a basis of U_1. Similarly, $\{c_1,\ldots,c_k,b_{k+1},\ldots,b_m\}$ is a basis of U_2.

Now, we claim that $\{c_1,\ldots,c_k,a_{k+1},\ldots,a_n,b_{k+1},\ldots,b_m\}$ is a basis of U_1+U_2. Firstly, it's clear that this set spans U_1+U_2 since it spans both U_1 and U_2. Assume toward a contradiction that this set is not linearly independent. Then, there exist $x_1,\ldots,x_{n+m-k}$ not all zero such that

$$[x_1c_1+\cdots+x_kc_k]+[x_{k+1}a_{k+1}+\cdots+x_na_n]+[x_{n+1}b_{k+1}+\cdots+x_{n+m-k}b_m] = 0.$$

Define $a := [x_1c_1+\cdots+x_kc_k]+[x_{k+1}a_{k+1}+\cdots+x_na_n]$. Clearly $a \in U_1\setminus\{0\}$, because if $a=0$ this would contradict the linear independence of $\{c_1,\ldots,c_k,a_{k+1},\ldots,a_n\}$. Now,

$$-a = [x_{n+1}b_{k+1}+\cdots+x_{n+m-k}b_m]$$

and so $a \in U_2$. Hence, $a \in [U_1\cap U_2]\setminus\{0\}$ and so we can write a as

$$a = y_1c_1+\cdots+y_kc_k.$$

with $\{y_1,\ldots,y_k\}$ not all zero.

Finally,

$$0 = -a+a = x_{n+1}b_{k+1}+\cdots+x_{n+m-k}b_m+y_1c_1+\cdots+y_kc_k.$$

Since $\{x_{n+1}, \ldots, x_{n+m-k}, y_1, \ldots, y_k\}$ not all zero, this contradicts the fact that $\{c_1, \ldots, c_k, b_{k+1}, \ldots, b_m\}$ is a basis of U_2 and hence linearly independent.

Therefore, the set $\{c_1, \ldots, c_k, a_{k+1}, \ldots, a_n, b_{k+1}, \ldots, b_m\}$ is linearly independent, and so it is a basis of $U_1 + U_2$ of cardinality $n + m - k$.

So, we have verified that

$$\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2). \ \square$$

78 Suppose that $T : V \to W$ is a linear transformation between vector spaces over the same field F. Prove that T is one-to-one precisely when it maps linearly independent sets to linearly independent sets.

Proof:

($\Longrightarrow$) :

Let T be one-to-one. Let $\{x_1, \ldots, x_n\} \subseteq V$ be a linearly independent set. We need to show that $\{T(x_1), \ldots, T(x_n)\}$ is a linearly independent set.

Let $a_1, \ldots, a_n$ be such that

$$a_1 T(x_1) + \cdots + a_n T(x_n) = 0.$$

Then, by the properties of linear transformations (recall that a linear transformation over a vector space F is just a special F-module homomorphism), we have that

$$T(a_1 x_1 + \cdots + a_n x_n) = 0.$$

Since T is one-to-one, we have that

$$a_1 x_1 + \cdots + a_n x_n = 0,$$

and by the linear independence of $\{x_1, \ldots, x_n\}$, we conclude that

$$a_1 = a_2 = \cdots = a_n = 0.$$

Therefore, the set $\{T(x_1), \ldots, T(x_n)\}$ is linearly independent, and so T maps linearly independent sets to linearly independent sets. $\square$

($\Longleftarrow$) :

Let T map linearly independent sets to linearly independent sets. Let $v \in V$ be nonzero. Then, $\{v\}$ is a linearly independent set. By assumption, the set $\{T(v)\}$ is linearly independent, from which we conclude that $T(v) \neq 0$, because $\{0\}$ is not a linearly independent set. So, we have shown that $\mathrm{Ker}(T) = \{0\}$, and hence R is one-to-one. $\square$

79 Suppose that $T : V \to V$ is a linear transformation on the vector space V. Call T a *projection* if $T^2 = T$. Prove that if T is a projection then $V = \mathrm{Ker}(T) \oplus \mathrm{Im}(T)$. Give an example to show that the converse is false.

Proof:

To show that $V = \mathrm{Ker}\, T \oplus \mathrm{Im}\, T$, we need to show that

(1) $\mathrm{Ker}(T) \cap \mathrm{Im}(T) = \{0\}$,

(2) For all $v \in V$, there exist $v_1 \in \text{Ker}(T)$ and $v_2 \in \text{Im}(T)$ such that $v = v_1 + v_2$.

Let $w \in \text{Im}(T)$ be nonzero. Then, $w = T(v)$ for some nonzero $v \in V$. Now, $T(w) = T(T(v)) = T(v) = w \neq 0$. So, $T(w) \neq 0$ and hence $w \notin \text{Ker}(T)$. Thus $\text{Im}(T) \cap \text{Ker}(T) = 0$.

Now, let $v \in V$. Define $v_1 := T(v) \in \text{Im}(T)$ and $v_2 := v - T(v)$. Note that $T(v_2) = T(v - T(v)) = T(v) - T(T(v)) = T(v) - T(v) = 0$, so that $v_2 \in \text{Ker}(T)$.

Since $v_1 + v_2 = T(v) + (v - T(v)) = v$, we have shown that $V = \text{Im}(T) \oplus \text{Ker}(T)$. $\square$

For a counterexample, let $V = \mathbb{R}$ and T be multiplication by -1. In this case, $\text{Ker}(T)$ is empty, and $V = \text{Im}(T)$, yielding $V = \text{Ker}(T) \oplus \text{Im}(T)$. However, $T^2 = \text{Id} \neq T$.

80 Suppose that V is a finite dimensional vector space over the field F and that $T : V \to W$ is a linear transformation into a vector space W over F. Prove that

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T)).$$

Proof:

Let $|V| = n < \infty$. Pick an arbitrary set of $n + 1$ elements in $\text{Im}(T)$.:

$$\{T(v_1), \ldots, T(v_{n+1})\}.$$

Note that the set $\{v_1, \ldots, v_{n+1}\}$ is not linearly independent, so we can write

$$v_{n+1} = \sum_{i=1}^{n} a_i v_i,$$

where $\{a_i\}$ are not all zero. Thus

$$T(v_{n+1}) = \sum_{i=1}^{n} a_i T(v_i),$$

and so the set $\{T(v_1), \ldots, T(v_{n+1})\}$ is not linearly independent. Therefore,

$$\dim(\text{Im}(T)) \leq \dim(V) < \infty.$$

Now, we show that $\dim(V) = \dim(\text{Ker}(T)) + \dim(V/\text{Ker}(T))$. Let $\{v_1, \ldots, v_n\}$ be a basis of V and let $\{w_1, \ldots, w_k\}$ be a basis of $\text{Ker}(T)$ with $k \leq n$ (we know that $\text{Ker}(T)$ has a finite basis because it is a subspace of V). By the replacement theorem, $\{w_1, \ldots, w_k, v_{k+1}, \ldots, v_k\}$ is a basis of V.

Consider the natural projection map $\varphi : V \to V/\text{Ker}(T)$. Note that $\varphi(w_i) = 0$ for all i.

Assume toward a contradiction that

$$\varphi(a_{k+1}v_{k+1} + \cdots + a_n v_n) = 0.$$

This would imply that $a_{k+1}v_{k+1} + \cdots + a_n v_n \in \text{Ker}(T)$, which is a contradiction. Hence, $V/\text{Ker}(T)$ is spanned by $\{v_{k+1}, \ldots, v_n\}$, which is a linearly independent set. So, $\dim(V/\text{Ker}(T)) = n - k$.

Since $V/\text{Ker}(T) \cong \text{Im}(T)$ by the First Isomorphism Theorem of modules, we conclude that

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T)). \ \square$$

81 Obtain a formula for the number of one dimensional subspaces of an n dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$ of p elements (where p is a prime number). Justify your choice.

Proof:

A one dimensional subspace of $(\mathbb{Z}/p\mathbb{Z})^n$ is generated by a single nonzero vector. The number of nonzero vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ is $p^n - 1$. However, for each one dimensional subspace, there are a total of $p - 1$ vectors that generate the same subspace. Therefore, the number of distinct one dimensional subspaces of an n dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ is

$$\frac{p^n - 1}{p - 1} = p^{n-1} + p^{n-2} + \cdots + p^2 + p + 1. \ \square$$

82 (a) Define: *Irreducible module* over a ring R with identity.

(b) Now assume that R is commutative as well. Prove that the R-module M is irreducible if and only if $M \cong R/I$ for some maximal ideal I of R. Use this to classify the irreducible $\mathbb{Z}$-modules.

Part (a):

An R-module M is *irreducible* if $M \neq 0$ and 0 and M are the only submodules of M.

Proof of (b):

Lemma: M is irreducible if and only if M is cyclic with each nonzero element as a generator.
Proof:

$(\Longrightarrow)$:

Let M be irreducible. Let $a \in M$ be nonzero. Since $Ra = \{ra \mid r \in R\}$ is a submodule of M, we have that either $Ra = 0$ or $Ra = M$. But, $Ra \neq 0$ because $1 \in R$ and $1 \cdot a = a \neq 0$. Thus, $Ra = M$, and so M is cyclic with each nonzero element as a generator. $\square$

$(\Longleftarrow)$:

Assume toward a contradiction that M is cyclic with every nonzero element as a generator, but that M is not irreducible. Then, there exists a nontrivial proper submodule N. Let $a \in N$ be nonzero. Then, $Ra = M$ by assumption, and so $N = M$, a contradiction. Therefore M is irreducible. $\square$

$(\Longrightarrow)$:

Let M be irreducible. Let $m \in M$ be nonzero. Define a map $\varphi : R \to M$ by $r \mapsto rm$. Note that φ is a homomorphism, since $\varphi(x + ry) = (x + ry)m = xm + r(ym) = \varphi(x) + r\varphi(y)$. Now, by the **Lemma**, we have that $\operatorname{Im}\varphi = M$, and so φ is surjective.

To see that $\operatorname{Ker}\varphi$ is a maximal ideal, let $x + \operatorname{Ker}\varphi$ be nonzero so that $xm \neq 0$. Since M is irreducible, we have that $M = R(xm)$. Thus $m = y(xm) = (yx)m$ for some $y \in R$. Hence $1m - (yx)m = 0$ and so $1 - yx \in \operatorname{Ker}\varphi$. So, we see that $(y + \operatorname{Ker}\varphi)(x + \operatorname{Ker}\varphi) = 1 + \operatorname{Ker}\varphi$. We have shown that every nonzero element in $R/\operatorname{Ker}\varphi$ has a left inverse (and hence a two-sided inverse because R is commutative), and thus $\operatorname{Ker}\varphi$ is a maximal ideal. By the First Isomorphism Theorem of modules, we have that $M \cong R/\operatorname{Ker}\varphi$, and so the theorem holds. $\square$

($\Longleftarrow$) :

Let $M \cong R/I$ for some maximal ideal I. Let $x + I$ be nonzero. Since R/I is a field, there exists $y \in R$ such that $(y + I)(x + I) = 1 + I$. Let $r + I \in R/I$, and observe that $r + I = (ry + I)(x + I)$. Therefore, $r + I \in R(x + I)$, and so $R/I = R(x + I)$, i.e., R/I is generated as an R-module by any nonzero element. By the **Lemma**, this means that R/I is an irreducible R-module, and hence M is an irreducible R-module. □

Recall that the $\mathbb{Z}$-modules are exactly the abelian groups, and so the $\mathbb{Z}$-submodules are exactly the subgroups of the abelian groups. If M is an irreducible $\mathbb{Z}$-module, then it's only submodules are 0 and M, and so as an abelian group its only subgroups are the trivial subgroup and itself. Therefore, as an abelian group, it is cyclic and generated by every nonzero element. This implies that as an abelian group, it is cyclic of prime order. Conversely, an abelian group that is cyclic of prime order is clearly an irreducible $\mathbb{Z}$-module. Therefore, the irreducible $\mathbb{Z}$-modules are exactly the cyclic groups of prime order.

83 Prove **Schur's Lemma**: Suppose that M is an irreducible module; then every nonzero endomorphism of M is an automorphism. Show how one concludes from this that if M is irreducible then $\mathrm{End}(M)$ is a division ring.

Proof:

Let M be an irreducible module. Let $\varphi : M \to M$ be a nonzero endomorphism. By definition φ is a homomorphism. Recall that $\mathrm{Ker}\,\varphi$ and $\mathrm{Im}\,\varphi$ are submodules of M. Since M is irreducible, each of $\mathrm{Ker}\,\varphi$ and $\mathrm{Im}\,\varphi$ is either 0 or M. Since φ is a nonzero endomorphism, we must have that $\mathrm{Ker}\,\varphi = 0$ and $\mathrm{Im} = M$. Hence, φ is both injective and surjective, and therefore an isomorphism. So, φ is an automorphism of M.

A division ring is a ring in which every nonzero element has an inverse. (The difference between a division ring and a field is that a division ring need not be commutative.) Let $\varphi \in \mathrm{End}(M)$ be nonzero. By the above argument, φ is actually an isomorphism, and hence there exists a function $\varphi^{-1} \in \mathrm{End}(M)$ such that $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathrm{Id}_M$. Hence $\mathrm{End}(M)$ is a division ring (though not necessarily a field). □

84 Let R be a ring with identity. Suppose that $\varphi : M \to F$ is a surjective R-module homomorphism and that F is a free R-module. Prove that $M = \mathrm{Ker}\,\varphi \oplus N$, where $N \cong F$.

Proof:

Let $X \subseteq F$ be a basis of F. Since φ is surjective, for each $x \in X$ there exists $m_x \in M$ such that $\varphi(m_x) = x$. Then, by the **Universal Mapping Property of Modules**, the map $f : X \to M$ defined by $f(x) := m_x$ can be extended to a (unique) R-module homomorphism $\widehat{f} : F \to M$. Let $N := \mathrm{Im}\,\widehat{f}$.

Let $x \in X$. Note that $\varphi(\widehat{f}(x)) = \varphi(f(x)) = \varphi(m_x) = x$, for all $x \in X$, and hence $\varphi \circ \widehat{f} = \mathrm{Id}_X$. Let $a \in F$ be written as $a = \sum a_x x$. Then, $\varphi(\widehat{f}(a)) = \varphi\left(\widehat{f}\left(\sum a_x x\right)\right) = \sum a_x \varphi(\widehat{f}(x)) = \sum a_x x$, and thus $\varphi \circ \widehat{f} = \mathrm{Id}_F$.

Let $m \in M$ be arbitrary. Since $\varphi(m) \in F$ we have that $\widehat{f}(\varphi(m)) \in \operatorname{Im} \widehat{f} = N$. Additionally,

$$\begin{aligned}\varphi(m - \widehat{f}(\varphi(m))) &= \varphi(m) - \varphi(\widehat{f}(\varphi(m))) \\ &= \varphi(m) - (\varphi \circ \widehat{f})(\varphi(m)) \\ &= \varphi(m) - \mathrm{Id}_F(\varphi(m)) \\ &= \varphi(m) - \varphi(m) = 0.\end{aligned}$$

Thus, $m - \widehat{f}(\varphi(m)) \in \operatorname{Ker} \varphi$.

So, for $m \in M$, we can write $m = [m - \widehat{f}(\varphi(m))] + [\widehat{f}(\varphi(m))]$, with the first component in $\operatorname{Ker} \varphi$ and the second component in N.

Next, we need to show that $\operatorname{Ker} \varphi \cap \operatorname{Im} \widehat{f} \neq \{0\}$. Let $m \in \operatorname{Ker} \varphi$ be nonzero, so that $\varphi(m) = 0$. Assume toward a contradiction that $m \in \operatorname{Im} \widehat{f}$. Then, there exist a_x not all zero such that $m = \widehat{f}\left(\sum a_x x\right) = \sum a_x \widehat{f}(x)$. Now,

$$0 = \varphi(m) = \varphi\left(\sum a_x \widehat{f}(x)\right) = \sum a_x (\varphi \circ \widehat{f})(x) = \sum a_x x,$$

which contradicts the linear independence of the basis X. Thus, $m \notin \operatorname{Im} \widehat{f}$, and so

$$\operatorname{Ker} \varphi \cap N = \{0\}.$$

Lastly, it remains to show that $\operatorname{Im} \widehat{f} \cong F$. Assume toward a contradiction that $\operatorname{Ker} \widehat{f}$ is not trivial. Let $a \in \operatorname{Ker} \widehat{f}$ be nonzero. Write a as $\sum a_x x$. Then $0 = \widehat{f}\left(\sum a_x x\right) = \sum a_x \widehat{f}(x) = \sum a_x m_x$. Thus, $0 = \varphi(0) = \sum a_x \varphi(m_x) = \sum a_x x$, for a_x not all zero, which contradicts the linear independence of the basis X. Therefore $\operatorname{Ker} \widehat{f}$ is trivial. Hence, by the **First Isomorphism Theorem of Modules**, we have that $F \cong \operatorname{Im} \widehat{f}$. $\square$

85 Let R be a principal ideal domain and M be a torsion R-module. Define *primary module* and prove that M is isomorphic to a direct sum of primary R-modules.

Proof:

Let p be prime in R. The p-primary component of M is the set of all elements of M that are annihilated by some positive power of p. We will show that M is isomorphic to the (possibly infinite) direct sum of each p-primary component of M as p runs through all primes of R.

Define M_p to be the p-primary component of M, i.e.

$$M_p = \{m \in M \mid p^k m = 0, \text{ for some } k \in \mathbb{N}\}.$$

First we show that M_p is a submodule of M. Define

$$\operatorname{Ann}_M(\ell) := \{m \in M \mid \ell m = 0,$$

and note that

$$M_p = \bigcup_{k=0}^{\infty} \operatorname{Ann}_M(p^k).$$

First, we claim that $\operatorname{Ann}_M(\ell)$ is a submodule of M for all $\ell \in R$ (see proof below). Next, we claim that the union of a chain of submodules is a submodule (see proof below), and so since $\operatorname{Ann}_M(p^k) \subseteq \operatorname{Ann}_M(p^{k+1})$ this is a chain, and hence M_p is a submodule of M.

Now, we show that

$$M \cong \bigoplus_{\substack{p \in R \\ p \text{ prime}}} M_p.$$

Let p and q be distinct primes in R. We will show that $M_p \cap M_q = 0$. Let $m \in M_p \cap M_q$. Then, there exists k and ℓ such that $p^k \cdot m = q^\ell \cdot m = 0$. So, for every element $a \in (p^k,\ q^\ell)$ we must have that $a \cdot m = 0$. Since p and q are relatively prime, we have that $(p^k,\ q^\ell) = R$ and so $1 \in (p^k,\ q^\ell)$. Therefore, $m = 1 \cdot m = 0$.

Lastly, we show that every element $m \in M$ can be written as a finite sum $\sum m_{p_i}$ where $m_{p_i} \in M_{p_i}$ and p_i are distinct primes in R. Pick $m \in M$. Since M is torsion, we can pick $a \in R$ such that $a \cdot m = 0$. Factor a into primes as

$$a = \prod_{i \in T} p_i^{k_i},$$

where T is a finite set, and define

$$q_t := \prod_{\substack{i \in T \\ i \neq t}} p_i^{k_1}.$$

Since no prime divides all of the q_t terms, we have that the ideal generated by the set $\{q_t \mid t \in T\}$ is the whole ring R and this contains 1. So we can pick $\{x_t \mid t \in T\}$ from R such that

$$1 = \sum_{t \in T} x_t q_t.$$

Hence,

$$m = 1 \cdot m = \left(\sum_{t \in T} x_t q_t \right) m = \sum_{t \in T} \left(x_t q_t m \right).$$

For a particular $t \in T$ note that

$$p_t^{k_t} \cdot (x_t q_t m) = (p_t^{k_t} q_t) \cdot (x_t m) = x_t (a \cdot m) = 0,$$

and therefore $x_t q_t m \in M_{p_t}$.

So, we have shown that M is isomorphic to the direct sum of the primary components of M. □

86 Suppose that V is a finite dimensional vector space over the field F and that T is a linear transformation on V, so that the induced module action of $F[x]$ on V defines a cyclic module with cyclic vector w. Prove that:

(a) The set $\{w, T(w), T^2(w), \ldots, T^k(w)\}$ is a basis for a suitable k.

(b) Compute the matrix of T relative to this basis, pointing out the relationship which the entries of this matrix and k have to the monic polynomial in $F[x]$ that generates the annihilator of w.

(c) Compute the characteristic polynomial of the matrix in (b).

Proof of (a):

Let the induced module action of $F[x]$ on V define a cyclic module with cyclic vector w, i.e.,

$$F[x] \cdot V = F[x] \cdot w.$$

Let k be maximal such that the set $\{w, T(w), T^2(w), \ldots, T^k(w)\}$ is linearly independent. Since the $k = 1$ case is always linearly independent, we have $k \geq 1$. Let $v \in V$ as an $F[x]$-module. Then, $v = p(x) \cdot w = [p(T)](w)$ for some $p(x) \in F[x]$. Note that since k is maximal, we have that $T^{k+1}(w)$ can be generated by the smaller powers of T, and therefore, we can pick $p(x)$ to have degree $\leq k$. Hence, the given set also spans V, and so is a basis. □

Proof of (b):

To compute the matrix of T relative to the given basis, we apply T to each element of the basis, and then express the result as a linear combination of the basis elements, and make this the corresponding column of the matrix. Hence, for $n < k$, we have that $T(T^n(w)) = T^{n+1}(w)$, which is expressed in terms of the basis as a column with a one in the $n+1^{\text{th}}$ spot and zeros elsewhere. Additionally, we can express $T^{k+1}(w)$ as a linear combination of the elements in the basis, so say that $T^{k+1}(w) = a_0 w + a_1 T(w) + \cdots + a_k T^k(w) = [q(T)](w)$, where $q(x) = a_0 + a_1 x + \cdots + a_k x^k$. Therefore, the matrix of T relative to the given basis is:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ 0 & 0 & 1 & \cdots & 0 & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_k \end{pmatrix}$$

The annihilator of w is the ideal of $F[x]$ for which $f(x) \cdot w = 0$ for all $f(x)$ in the ideal since $F[x]$ is a principal ideal domain, the ideal can be written as $(p(x))$, where $p(x)$ is the monic polynomial of least degree in the ideal. Note that the degree of $p(x)$ must be at least $k+1$, and in fact the polynomial

$$x^{k+1} - a_k x^k - a_{k-1} x^{k-1} - \cdots - a_1 x - a_0.$$

satisfies this requirement. □

Proof of (c):

The polynomial above

$$p(x) = x^{k+1} - a_k x^k - a_{k-1} x^{k-1} - \cdots - a_1 x - a_0$$

is both the minimal and the characteristic polynomials of T. To see this, note that the matrix representing T is already in rational canonical form, with one invariant factor. □

87 Suppose that T is a linear transformation on a finite dimensional vector space V, over a field F. Prove that T is diagonalizable if and only if $m_T(x)$, the minimum polynomial of T, can be factored as

$$m_T(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k),$$

where the $\lambda_i \in F$ $(i = 1, \ldots, k)$ are distinct.

Proof:

($\Longrightarrow$):

Let A be the matrix associated to T. Let B be the Jordan Canonical Form of A, which is diagonal by assumption. The Jordan blocks of B must be 1×1 since B is diagonal. Since the minimal polynomial of B is the least common multiple of the minimal polynomials of the Jordan blocks, we have that the minimal polynomial of B has no repeated roots. Recall that similar matrices have the same minimal polynomial. Therefore A (and T) have no repeated roots in their minimal polynomial, and so it can be written as

$$m_T(x) = (x - \lambda_1) \cdots (x - \lambda_k),$$

where the λ_i are distinct. □

($\Longleftarrow$):

Let

$$m_T(x) = (x - \lambda_1) \cdots (x - \lambda_k),$$

where the λ_i are distinct. Let B be the Jordan Canonical form of A. The eigenvalues of T are exactly the roots of the characteristic polynomial of B, which are exactly the roots of the minimal polynomial of B. Since $m_T(x)$ is the least common multiple of the minimal polynomials of the Jordan blocks of B, each Jordan block has minimal polynomial of the form $(x - \lambda_i)^1$ for some i. (This is because the minimal polynomial of a Jordan block has the form $(x - \lambda_i)^r$, and so $r = 1$.) Hence, each Jordan block is 1×1 and so B is diagonal. Therefore A is diagonalizable. $\square$

88 Suppose that A is a nilpotent 6×6 matrix over a field. Find all possible Jordan Canonical forms of A. Justify your arguments.

Proof:

Let A be a nilpotent matrix. Then, $A^k = 0$ for some k. In fact, we know for sure that $A^6 = 0$, since for a nilpotent $n \times n$ matrix N, we always have that $N^n = 0$. The characteristic polynomial $\chi_A(x)$ of A must have degree 6 and satisfy the equation $\chi_A(A) = 0$. Recall that the roots of the characteristic polynomial are exactly the eigenvalues of A. If λ is an eigenvalue of A, then for some nonzero $v \in V$, we have that $Av = \lambda v$, and so $A^2 v = \lambda^2 v$, and so on until $0 = A^6 v = \lambda^6 v$. Therefore $\lambda = 0$. Since λ was an arbitrary eigenvalue, we have that

$$\chi_A(x) = (x - 0)(x - 0)(x - 0)(x - 0)(x - 0)(x - 0) = x^6.$$

Now, the possible minimal polynomials of A are the divisors of $\chi_A(x)$, i.e.,

$$m_A(x) \in \{x, x^2, x^3, x^4, x^5, x^6\}.$$

From this we derive the possible invariant factor lists.

$m_A(x)$	x^6	x^5	x^4
Factor Lists	(1) x^6	(2) x^5, x	(3) x^4, x^2 (4) x^4, x, x
$m_A(x)$	x^3	x^2	x^1
Factor Lists	(5) x^3, x^3 (6) x^3, x^2, x (7) x^3, x, x, x	(8) x^2, x^2, x^2 (9) x^2, x^2, x, x (10) x^2, x, x, x, x	(11) x, x, x, x, x, x

These correspond to the Jordan Canonical Forms:

$$(1): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (2): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (3): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$(4): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (5): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (6): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$(7): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (8): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (9): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$(10): \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (11): \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

89 Prove that in $GL_2(\mathbb{Q})$ all the elements of order four are conjugate. (Hint: Consider the rational canonical form of such an element.)

Proof:

Let $A \in GL_2(\mathbb{Q})$ have order 4, so that $A^4 = 1$ but $A^2 \neq 1$. Then, we have that

$$A^4 - \mathrm{Id} = 0$$

and so

$$(A^2 + 1)(A + 1)(A - 1) = 0.$$

Let $\chi_A(x)$ be the characteristic polynomial of A. Recall that $\deg(\chi_A(x)) = 2$. By the order condition, we have that

$$\chi_A(x) \mid (x^4 - 1) \qquad \text{and } \chi_A(x) \nmid (x^2 - 1).$$

Hence, $\chi_A(x) = x^2 + 1$. Since $\chi_A(x)$ is irreducible in $\mathbb{Q}$ and because the minimal polynomial $m_A(x)$ of A divides $\chi_A(x)$ and has degree at least one we see that $m_A(x) = \chi_A(x)$.

Recall that for 2×2 and 3×3 matrices, two matrices are similar if and only if they have the same minimal and characteristic polynomials (this holds in only one direction for bigger matrices). Therefore, all elements of order four are similar (since we showed they must have the same minimal and characteristic polynomials), and so as elements in $GL_2(\mathbb{Q})$ they are conjugate.

Note that the rational canonical form that they share is:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \ \square$$

90 Suppose that V is a vector space of dimension 7 over the field of real numbers $\mathbb{R}$, and T is a linear transformation on V which satisfies $T^4 = I$. Compute the following:

(a) the possible minimum polynomials of T, and the characteristic polynomial that goes with each choice,

(b) the possible Rational Canonical Forms of T.

Proof:

Since we have that $T^4 = I$, it must be true that

$$T^4 - 1 = (T^2 + 1)(T + 1)(T - 1) = 0.$$

Hence, the possibilities for the minimal polynomial are:

$$\begin{array}{cccc} (T^2+1)(T+1)(T-1), & (T^2+1), & (T^2+1)(T+1), & (T^2+1)(T-1), \\ (T+1)(T-1), & (T+1), & (T-1). & \end{array}$$

Now, to find the possible characteristic polynomials for each possible minimal polynomial, we consider the possible invariant factor lists, keeping in mind that each invariant factor must divide its minimal polynomial, and the sum of the degrees of the whole list must equal the dimension of V, which is 7. Note that because of this, the minimal polynomial T^2+1 has zero possibilities, since any characteristic polynomial to which is belongs would have even degree. We have the following possibilities:

$m_T(x)$	Invariant Factors	$\chi_T(x)$
$(T^2+1)(T+1)(T-1)$	$(T^2+1)(T+1)(T-1)$, $(T^2+1)(T+1)$	$(T^2+1)^2(T+1)^2(T-1)^1$
	$(T^2+1)(T+1)(T-1)$, $(T^2+1)(T-1)$	$(T^2+1)^2(T+1)^1(T-1)^2$
	$(T^2+1)(T+1)(T-1)$, $(T+1)(T-1)$, $(T+1)$	$(T^2+1)^1(T+1)^3(T-1)^2$
	$(T^2+1)(T+1)(T-1)$, $(T+1)(T-1)$, $(T-1)$	$(T^2+1)^1(T+1)^2(T-1)^3$
	$(T^2+1)(T+1)(T-1)$, $(T+1)$, $(T+1)$, $(T+1)$	$(T^2+1)^1(T+1)^4(T-1)^1$
	$(T^2+1)(T+1)(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$	$(T^2+1)^1(T+1)^1(T-1)^4$
(T^2+1)	*none*	*none*
$(T^2+1)(T+1)$	$(T^2+1)(T+1)$, (T^2+1), (T^2+1)	$(T^2+1)^3(T+1)^1$
	$(T^2+1)(T+1)$, $(T^2+1)(T+1)$, $(T+1)$	$(T^2+1)^2(T+1)^3$
	$(T^2+1)(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$	$(T^2+1)^1(T+1)^5$
$(T^2+1)(T-1)$	$(T^2+1)(T-1)$, (T^2+1), (T^2+1)	$(T^2+1)^3(T-1)^1$
	$(T^2+1)(T-1)$, $(T^2+1)(T-1)$, $(T-1)$	$(T^2+1)^2(T-1)^3$
	$(T^2+1)(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$	$(T^2+1)^1(T-1)^5$
$(T+1)(T-1)$	$(T+1)(T-1)$, $(T+1)(T-1)$, $(T+1)(T-1)$, $(T+1)$	$(T+1)^4(T-1)^3$
	$(T+1)(T-1)$, $(T+1)(T-1)$, $(T+1)(T-1)$, $(T-1)$	$(T+1)^3(T-1)^4$
	$(T+1)(T-1)$, $(T+1)(T-1)$, $(T+1)$, $(T+1)$, $(T+1)$	$(T+1)^5(T-1)^2$
	$(T+1)(T-1)$, $(T+1)(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$	$(T+1)^2(T-1)^5$
	$(T+1)(T-1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$	$(T+1)^6(T-1)^1$
	$(T+1)(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$	$(T+1)^1(T-1)^6$
$(T+1)$	$(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$, $(T+1)$	$(T+1)^7$
$(T-1)$	$(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$, $(T-1)$	$(T-1)^7$

Now, we give the rational canonical form of each of these (presented from left to right then up to down) in the same order in the given list.

$(T^2+1)(T+1)(T-1),\ (T^2+1)(T+1)$:

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

$(T^2+1)(T+1)(T-1),\ (T^2+1)(T-1)$:

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

$(T^2+1)(T+1)(T-1),\ (T+1)(T-1),\ (T+1)$:

$$\begin{pmatrix} \begin{pmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{pmatrix} & & \\ & \begin{pmatrix} 0&1\\1&0 \end{pmatrix} & \\ & & (-1) \end{pmatrix} = \begin{pmatrix} 0&0&0&1&0&0&0\\1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&1&0&0\\0&0&0&0&0&0&-1 \end{pmatrix}$$

$(T^2+1)(T+1)(T-1),\ (T+1)(T-1),\ (T-1)$:

$$\begin{pmatrix} \begin{pmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{pmatrix} & & \\ & \begin{pmatrix} 0&1\\1&0 \end{pmatrix} & \\ & & (1) \end{pmatrix} = \begin{pmatrix} 0&0&0&1&0&0&0\\1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&0&1&0\\0&0&0&0&1&0&0\\0&0&0&0&0&0&1 \end{pmatrix}$$

$(T^2+1)(T+1)(T-1),\ (T+1),\ (T+1),\ (T+1)$:

$$\begin{pmatrix} \begin{pmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{pmatrix} & & & \\ & (-1) & & \\ & & (-1) & \\ & & & (-1) \end{pmatrix} = \begin{pmatrix} 0&0&0&1&0&0&0\\1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&-1&0&0\\0&0&0&0&0&-1&0\\0&0&0&0&0&0&-1 \end{pmatrix}$$

$$(T^2+1)(T+1)(T-1),\ (T-1),\ (T-1),\ (T-1):$$

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

$$(T^2+1)(T+1),\ (T^2+1),\ (T^2+1):$$

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

$$(T^2+1)(T+1),\ (T^2+1)(T+1),\ (T+1):$$

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

$$(T^2+1)(T+1),\ (T+1),\ (T+1),\ (T+1),\ (T+1):$$

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

$$(T^2+1)(T-1),\ (T^2+1),\ (T^2+1):$$

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

$(T^2+1)(T-1),\ (T^2+1)(T-1),\ (T-1):$

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

$(T^2+1)(T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1):$

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

$(T+1)(T-1),\ (T+1)(T-1),\ (T+1)(T-1),\ (T+1)$

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

$(T+1)(T-1),\ (T+1)(T-1),\ (T+1)(T-1),\ (T-1)$

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

$(T+1)(T-1),\ (T+1)(T-1),\ (T+1),\ (T+1),\ (T+1)$

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

$$(T+1)(T-1),\ (T+1)(T-1),\ (T-1),\ (T-1),\ (T-1)$$

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

$$(T+1)(T-1),\ (T+1),\ (T+1),\ (T+1),\ (T+1),\ (T+1)$$

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

$$(T+1)(T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1)$$

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

$$(T+1),\ (T+1),\ (T+1),\ (T+1),\ (T+1),\ (T+1),\ (T+1)$$

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

$$(T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1),\ (T-1)$$

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

91 Suppose that V is a finite dimensional vector space over $\mathbb{Q}$, and T is an invertible linear transformation on V for which $T^{-1} = T^2 + T$. Prove:

(a) The dimension of V is a multiple of 3.

(b) If the dimension is 3, prove that all such transformations are similar.

Proof of (a):

Let $T^{-1} = T^2 + T$. Then, for any $v \in V$, we have that

$$T^{-1}(v) = T^2(v) + T(v).$$

Hence,

$$T^0(v) = v = T(T^2(v) + T(v)) = T^3(v) + T(v),$$

and so

$$T^3(v) + T(v) - T^0(v) = 0.$$

Therefore, the minimal polynomial $m_T(x)$ of T must divide $x^3 + x^2 - 1$, which is irreducible because it clearly has no linear factors because it has no integer roots. Hence, $m_T(x) = x^3+x^2-1$. Now, each of the invariant factors must divide $m_T(x)$, and they cannot be constant. Therefore, the characteristic polynomial $\chi_T(x)$ of T is some positive power of $m_T(x)$, i.e.,

$$\chi_T(x) = (m_T(x))^k = (x^3 + x^2 - 1)^k,$$

for some positive integer k. So, $\deg(\chi_T(x)) = 3k$. Since the degree of the characteristic polynomial is the dimension of V (and V is finite), we have that $3 \mid \dim(V)$. □

Proof of (b):

Now let $k = 1$ so that

$$\chi_T(x) = m_T(x) = x^3 + x^2 - 1.$$

Since this is the only possibility, all such transformations have the same minimal and characteristic polynomials. Recall that any two 3×3 matrices with the same minimal and characteristic polynomials are similar (see **Exercise 93**). Therefore, the matrices representing any two such transformations are similar, and consequently any two such transformations are similar. □

92 Consider the statement:

All 3×3 matrices $A \neq I$ with real entries, such that $A^3 = I$ are similar over $\mathbb{R}$.

Prove or disprove.

Proof:

Let A be a matrix over $\mathbb{R}$ satisfying $A^3 = I$ and $A \neq I$. So, A satisfies the equation $x^3 - 1 = 0$. Hence, the minimal polynomial $m_A(x)$ of A must divide the polynomial $x^3-1 = (x-1)(x^2+x+1)$. Firstly, $m_A(x)$ cannot be constant. Additionally, $m_A(x) \neq 1$ because A satisfies its own minimal polynomial, which would imply $A = I$. Next, $m_A(x) \neq (x^2 + x + 1)$, because in this case we cannot construct a characteristic polynomial of degree three that is divisible by $m_A(x)$. Hence, we must have that $m_A(x) = \chi_A(x) = x^3 - 1$. By the fact that any two 3×3 matrices with the same minimal and characteristic polynomials are similar, and since we showed that there is only one possibility, we have that any two such matrices are similar. □

93 Prove, over any field F, that if two 2×2 matrices or two 3×3 matrices have the same minimum and characteristic polynomials then they are similar matrices. Give an example which shows that this is false for matrices of greater dimension.

Proof:

Let A and B be 2×2 matrices over the field F such that $m(x) := m_A(x) = m_B(x)$ and $\chi(x) := \chi_A(x) = \chi_B(x)$. We need to show that given any particular choice of $m(x)$ and $\chi(x)$, there is only one possible invariant factor list.

Since $\deg(\chi(x)) = 2$, we have that either $\chi(x)$ is an irreducible of degree two, or reducible with two linear factors. In the first case, we have that $m(x) = \chi(x)$, and the invariant factor list is just: $m(x)$. In the second case, we can write $\chi(x)$ as $(x-a)(x-b)$, for $a, b \in F$, and now, $m(x) \in \{(x-a), (x-b), (x-a)(x-b)\}$. If $m(x) = (x-a)$, then the invariant factor list must be: $(x-a)$, $(x-a)$. Similarly if $m(x) = (x-b)$. Lastly, if $m(x) = (x-a)(x-b)$, then the invariant factor list has just one term: $m(x)$.

Hence, in all possible choices of $m(x)$ and $\chi(x)$, there is only one possible invariant factor list. Therefore, A and B must have the same rational canonical form and consequently A and B are similar. □

If there is only one invariant factor, then it is $m(x)$ and so $m(x)$ has degree 3. If there are two invariant factors, then $m(x)$ must have degree 2 and there is some root r such that $c(x) = (x-r)m(x)$. Since the first invariant factor must divide $m(x)$ and the second invariant factor must be $m(x)$, we get that the invariant factor list is $x-r$, $m(x)$. If there are three invariant factors, then they must all have degree 1, and in fact must be equal. So, there is some root r such that $m(x) = x-r$, and the invariant factor list is $x-r$, $x-r$, $x-r$.

Since there cannot be more than three invariant factors (and there must be at least one), we have shown that in all such cases, there is only one possibility for the invariant factor list. Hence, A and B have the same invariant factors. We now see that A and B have the same rational canonical form, since the rational canonical form follows directly from the invariant factors. Since two matrices with the same rational canonical form are similar, we have that A and B are similar. □

Consider matrices A and B sharing characteristic polynomial $(x+1)^4$ and minimal polynomial $(x+1)^2$. Let A have invariant factor list $(x+1)^2, (x+1)^2$ and let B have invariant factor list $(x+1), (x+1), (x+1)^2$. Let A' be the rational canonical form of A and let B' be the rational canonical form of B.

Then, $A' = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -2 \end{pmatrix}$ and $B' = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -2 \end{pmatrix}$.

Since A and B do not have the same rational canonical form, we conclude that A and B are not similar, despite the fact that they have the same characteristic polynomial and the same minimal polynomials. □

94 On a vector space V of dimension 8 over the field $\mathbb{Q}$, T is a linear transformation for which the minimum polynomial is

$$m_T(x) = (x^2+1)^2(x-3).$$

Determine all possible Rational Canonical Forms. Justify your answer.

Proof:

The given minimal polynomial has degree 5. So, the sum of degrees of any other invariant factors

is 3. Therefore, the possible invariant factor lists are:

$$(x^2+1)^2(x-3),\ (x^2+1)(x-3),$$
$$(x^2+1)^2(x-3),\ (x-3),\ (x-3),\ (x-3).$$

Note that

$$(x^2+1)^2(x-3) = x^5 - 3x^4 + 2x^3 - 6x^2 + x - 3,$$

and

$$(x^2+1)(x-3) = x^3 - 3x^2 + x - 3.$$

So, the associated Rational Canonical Forms are:

$$\begin{pmatrix} \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix} & & \\ & \begin{pmatrix} 0 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix} \end{pmatrix},$$

$$\begin{pmatrix} (\ 3\ ) & & & \\ & (\ 3\ ) & & \\ & & (\ 3\ ) & \\ & & & \begin{pmatrix} 0 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix} \end{pmatrix}. \ \square$$

95 A *projection* is a linear transformation $P : V \to V$ on a vector space V for which $P^2 = P$. Assume that V has finite dimensional and prove the following:

(a) Any projection is diagonalizable.

(b) Two projections have the same diagonal form if and only if their kernels have the same dimension.

Proof of (a):

Since $P^2 = P$, we have that $P^2 - P = 0$, and so $P(P-1) = 0$. Hence, the minimal polynomial $m_P(x)$ of P must divide $x(x-1)$, and consequently $m_P(x)$ has no repeated roots. By **Exercise 87**, this implies that P is diagonalizable. $\square$

Proof of (b):

Let $n := \dim(V)$. Recall from **Exercise 79** for all projections T, we have that

$$\mathrm{Ker}(T) \cap \mathrm{Im}(T) = \{0\} \quad \text{and} \quad V = \mathrm{Ker}(T) \oplus \mathrm{Im}(T).$$

Let $k := \dim(\mathrm{Ker}(T))$. Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis for V. With some reordering, we can let $\mathcal{B}_1 := \{b_1, \ldots, b_k\}$ be a basis for $\dim(\mathrm{Ker}(T))$ and $\mathcal{B}_2 := \{b_{k+1}, \ldots, b_n\}$ be a basis for $\dim(\mathrm{Im}(T))$. We can do this splitting because each basis vector is either in $\mathrm{Ker}(T)$ or $\mathrm{Im}(T)$, and so each of the two basis parts are still linearly independent and spanning their respective subspaces.

Observe that if $v \in \mathrm{Im}(T)$, then $v = \varphi(v')$ for some $v' \in V$, and so

$$\varphi(v) = \varphi(\varphi(v')) = \varphi(v') = v = 1 \cdot v,$$

and so v is an eigenvector with eigenvalue 1.

Similarly, if $v \in \mathrm{Ker}(T)$, then

$$\varphi(v) = 0 = 0 \cdot v,$$

and so v is an eigenvector with eigenvalue 0.

Since every basis vector is an eigenvector the i^{th} column of the matrix representing T is $T(b_i) = \lambda_i$, where λ_i is the associated eigenvalue. Therefore, the matrix representing T is diagonal with k zeros and $n-k$ ones.

$(\Longleftarrow)$:

Let T and S be projections such that $\dim(\mathrm{Ker}(T)) = \dim(\mathrm{Ker}(S)) =: k$. Then, $\dim(\mathrm{Im}(T)) = \dim(\mathrm{Im}(S))$, and so by the above reasoning, T and S as matrices are both diagonal with k zeros and $n-k$ ones, and hence they have the same diagonal form. □

$(\Longrightarrow)$:

Let T and S be projections with the same diagonal form. As above, T and S as matrices have all zeros and ones along the diagonals, and the number of 0s is the dimension of the kernel of the respective projection. So, if T and S have the same diagonal form, we have that $\dim(\mathrm{Ker}(T)) = \dim(\mathrm{Ker}(S))$. □

96 Prove that there are exactly two conjugacy classes of 5×5 matrices with entries in $\mathbb{Q}$ for which $T^8 = 1$ and $T^4 \neq 1$.

Proof:

Since a transformation must satisfy its own minimal polynomial, we have that

$$m_T(x) \mid x^8 - 1 = (x^4+1)(x^2+1)(x+1)(x-1)$$

and

$$m_T(x) \nmid x^4 - 1 = (x^2+1)(x+1)(x-1).$$

Hence, since $\deg(m_T(x)) \leq 5$ and $m_T(x)$ must have a factor of (x^4+1), the only possibilities for the minimal polynomial of T are:

$$m_1(x) := (x^4+1)(x+1),$$

$$m_2(x) := (x^4+1)(x-1).$$

Since each has degree 5, it is the entire invariant factor list, and so the rational canonical forms, one that represents each conjugacy class (i.e., similarity class) are:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}. \ \square$$

97 T is a linear transformation on the n dimensional vector space V, over the field G, and there is a basis $\{v_1, \ldots, v_n\}$ for V for which $T(v_i) = v_{i+1}$, for $i = 1, 2, \ldots, n-1$ and $T(v_n) = v_1$. As a module over $F[x]$ with the action induced by T, show that

(a) V is a cyclic module but not irreducible.

(b) If $F = \mathbb{Q}$ and n is a prime number, prove that V is the direct sum of two irreducible $F[x]$-submodules, of dimensions 1 and $n-1$, respectively, over $\mathbb{Q}$.

Proof of (a):

Let $v \in V$ be expressible in terms of the basis as

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n = a_1v_1 + a_2T(v_1) + \cdots + a_nT^{n-1}(v_1) = p(x) \cdot v_1,$$

where $p(x) = a_1 + a_2x + \cdots + a_nx^{n-1} \in F[x]$. So V is cyclicly generated by v_1, i.e.

$$V = F[x] \cdot c_1.$$

To see that V is not irreducible, consider the submodule generated cyclicly by $v_1 + \cdots + v_n =: v$. Note that this element is fixed by T. Hence,

$$F[x] \cdot (v_1 + \cdots + v_n) = \{(a_1 + \cdots + a_n)v \mid a_1, \ldots, a_n \in F\} = \{av \mid a \in F\},$$

which is a one-dimensional subspace of V. Assuming that $n > 1$, this shows that V is not irreducible as an $F[x]$-module. □

Proof of (b):

Note that $T^n = \mathrm{Id}$ and so T satisfies the polynomial

$$x^n - 1 = (x-1)(x^{p-1} + \cdots + 1),$$

and so the minimal polynomial of T is one of the following possibilities:

$$\begin{aligned} m_1(x) &= x - 1, \\ m_2(x) &= x^{p-1} + \cdots + 1, \\ m_3(x) &= x^p - 1. \end{aligned}$$

$m_1(x)$ is not possible because $T \neq 1$ (under the assumption that $n > 1$), and $m_2(x)$ is not possible because no invariant factor list could sum to the proper degree. Hence the minimal polynomial of T is $m_3(x) = x^p - 1$. Hence, we have that

$$V \cong \mathbb{Q}[x]/(x^p - 1).$$

Since $\mathbb{Q}$ is a principal ideal domain, V is nonzero torsion with nonzero annihilator (a), where

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

Each of these factors is irreducible, and hence prime. So by the **Primary Decomposition Theorem**, we have that

$$V = N_1 \oplus N_2,$$

where $N_1 := \{v \in V \mid (x-1) \cdot v = 0\}$ and $N_2 := \{v \in V \mid (x^{p-1} + \cdots + 1) \cdot v = 0\}$. Additionally, $\dim(N_1) = n - 1$ and $\dim(N_2) = n - (n-1) = 1$. □

98 (a) Define the terms *eigenvector* and *eigenvalue* of a linear transformation T.

(b) Prove that the set of eigenvectors of T for which the corresponding eigenvalues are distinct must be linearly independent.

Proof of (a):

Let V be a vector space over F. A vector $v \in V$ is an eigenvector of T if $T(v) = \lambda v$ for some $\lambda \in F$. In this case, λ is an eigenvalue of T.

Proof of (b):

Let $\{v_1, \ldots, v_n\}$ be the set of eigenvectors of T for which the corresponding eigenvalues are distinct. Let the corresponding eigenvalues be $\{\lambda_1, \ldots, \lambda_n\}$.

Assume toward a contradiction that $\{v_1, \ldots, v_n\}$ is linearly dependent. Pick k to be the smallest possible positive integer such that $\{v_1, \ldots, v_k\}$ is linearly dependent (so that $\{v_1, \ldots, v_{k-1}\}$ is linearly independent). Note that $k > 1$, since every nonzero subset of size one is linearly independent.

So, there exist $a_1, \ldots, a_k$ not all zero such that

$$a_1 v_1 + \cdots + a_k v_k = 0. \tag{96.1}$$

Multiplying both sides of (96.1) by λ_k:

$$a_1 \lambda_k v_1 + \cdots + a_k \lambda_k v_k = 0. \tag{96.2}$$

Applying T to both sides of (96.1):

$$a_1 \lambda_1 v_1 + \cdots + a_k \lambda_k v_k = 0. \tag{96.3}$$

Subtracting (96.3) from (96.2):

$$a_1(\lambda_k - \lambda_1)v_1 + \cdots + a_{k-1}(\lambda_k - \lambda_{k-1})v_k = 0.$$

Note that each coefficient is nonzero by the assumption that the eigenvalues are distinct. Hence, the set $\{v_1, \ldots, v_{k-1}\}$ is linearly dependent, which contradictions the minimality of k. Therefore, the set $\{v_1, \ldots, v_n\}$ is linearly independent. □

99 Find one representative of each conjugacy class of elements of order 2 in the group $GL_5(\mathbb{F}_2)$ of invertible 5×5 matrices with entries in the field of two elements.

Proof:

First note that in $\mathbb{F}_2$, we have that $1 = -1$.

Let A be a matrix of order 2 in $GL_5(\mathbb{F}_2)$, then we have that A satisfies the polynomial

$$x^2 - 1 = x^2 + 1 = (x+1)^2 = 0.$$

Since A is not the identity, the minimal polynomial of A cannot be $x + 1$. Hence, the minimal polynomial must be $(x+1)^2$. Thus, the possible invariant factor lists are:

$$(x+1)^2, \ \ (x+1)^2, \ \ (x+1),$$

$$(x+1)^2, \ \ (x+1), \ \ (x+1), \ \ (x+1).$$

Represented as matrices in rational canonical form, the representatives for these two conjugacy classes, in order, are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \ \square$$

100 Let $GL_4(\mathbb{F}_3)$ denote the group of all invertible 4×4 matrices with entries in $\mathbb{F}_3$, the field of three elements. Use rational canonical forms to determine the number of conjugacy classes of elements of order 4. Give the rational canonical form for each class.

Proof:

Let A be a matrix of order 4 in $GL_4(\mathbb{F}_3)$. So, A satisfies the polynomial $x^4 - 1 = (x^2 + 1)(x + 1)(x + 2)$ and does not satisfy the polynomial $x^2 - 1 = (x + 1)(x + 2)$. Hence, the minimal polynomial of A contains a factor of $x^2 + 1$. The possibilities for minimal polynomial are:

$$(x^2 + 1)(x + 1)(x + 2),$$

$$(x^2 + 1)(x + 1),$$

$$(x^2 + 1)(x + 2),$$

$$(x^2 + 1).$$

Therefore, the possible invariant factor lists are:

(1) $(x^2 + 1)(x + 1)(x + 2)$

(2) $(x^2 + 1)(x + 1),\ \ (x + 1)$

(3) $(x^2 + 1)(x + 2),\ \ (x + 2)$

(4) $(x^2 + 1),\ \ (x^2 + 1)$

The corresponding rational canonical forms (noting $-1 = 2$ and $-2 = 1$) are:

$$\begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \ \square$$

101 Over $\mathbb{Q}$, compute the Jordan canonical form J of

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

Then, find a matrix S such that $J = SAS^{-1}$.

Proof:

First, we row reduce $xI - A$, keeping track of the row operations used. We use the operation "kill" to use the "1" entry in a column to zero out the rest of the row, using only column operations.

$$
\begin{aligned}
xI - A &= \begin{pmatrix} x-1 & -1 & -1 & -1 \\ 0 & x-1 & 0 & 1 \\ 0 & 0 & x-1 & -1 \\ 0 & 0 & 0 & x-1 \end{pmatrix} \\
&\xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} -1 & x-1 & -1 & -1 \\ x-1 & 0 & 0 & 1 \\ 0 & 0 & x-1 & -1 \\ 0 & 0 & 0 & x-1 \end{pmatrix} \\
&\xrightarrow{-C_1 \to C_1} \begin{pmatrix} 1 & x-1 & -1 & -1 \\ -(x-1) & 0 & 0 & 1 \\ 0 & 0 & x-1 & -1 \\ 0 & 0 & 0 & x-1 \end{pmatrix} \\
&\xrightarrow{R_2+(x-1)R_1 \to R_2} \begin{pmatrix} 1 & x-1 & -1 & -1 \\ 0 & (x-1)^2 & -(x-1) & -(x-2) \\ 0 & 0 & x-1 & -1 \\ 0 & 0 & 0 & x-1 \end{pmatrix} \\
&\xrightarrow{\text{kill}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & (x-1)^2 & -(x-1) & -(x-2) \\ 0 & 0 & x-1 & -1 \\ 0 & 0 & 0 & x-1 \end{pmatrix} \\
&\xrightarrow{C_2 \leftrightarrow C_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -(x-2) & -(x-1) & (x-1)^2 \\ 0 & -1 & x-1 & 0 \\ 0 & x-1 & 0 & 0 \end{pmatrix} \\
&\xrightarrow{R_2 \leftrightarrow R_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & x-1 & 0 \\ 0 & -(x-2) & -(x-1) & (x-1)^2 \\ 0 & x-1 & 0 & 0 \end{pmatrix} \\
&\xrightarrow{-C_2 \to C_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x-1 & 0 \\ 0 & x-2 & -(x-1) & (x-1)^2 \\ 0 & -(x-1) & 0 & 0 \end{pmatrix} \\
&\xrightarrow{R_3+(-(x-2))R_2 \to R_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x-1 & 0 \\ 0 & 0 & -(x-1)^2 & (x-1)^2 \\ 0 & -(x-1) & 0 & 0 \end{pmatrix} \\
&\xrightarrow{R_4+(x-1)R_2 \to R_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x-1 & 0 \\ 0 & 0 & -(x-1)^2 & (x-1)^2 \\ 0 & 0 & (x-1)^2 & 0 \end{pmatrix} \\
&\xrightarrow{\text{kill}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -(x-1)^2 & (x-1)^2 \\ 0 & 0 & (x-1)^2 & 0 \end{pmatrix} \\
&\xrightarrow{R_3 \leftrightarrow R_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & -(x-1)^2 & (x-1)^2 \end{pmatrix} \\
&\xrightarrow{R_4+R_3 \to R_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & 0 & (x-1)^2 \end{pmatrix}.
\end{aligned}
$$

Hence, the minimal polynomial is $(x-1)^2$ and the invariant factor list is

$$(x-1)^2,\ (x-1)^2.$$

Thus, the Jordan canonical form of A is:

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

The row operations used were:

(1) $R_2 + (x-1)R_1 \ \rightarrow \ R_2$

(2) $R_2 \ \leftrightarrow \ R_3$

(3) $R_3 + (-(x-2))R_2 \ \rightarrow \ R_3$

(4) $R_4 + (x-1)R_2 \ \rightarrow \ R_4$

(5) $R_3 \ \leftrightarrow \ R_4$

(6) $R_4 + R_3 \ \rightarrow \ R_4$

To find the matrix that conjugates A to its Jordan Canonical Form, we start with the 4×4 identity matrix and perform the following column operations corresponding to the above row operations:

(1) $C_1 - (A-1)C_2 \ \rightarrow \ C_1$

(2) $C_2 \ \leftrightarrow \ C_3$

(3) $C_2 + (A-2)C_3 \ \rightarrow \ C_2$

(4) $C_2 - (A-1)C_4 \ \rightarrow \ C_2$

(5) $C_3 \ \leftrightarrow \ C_4$

(6) $C_3 - C_4 \ \rightarrow \ C_3$

Note that

$$A - 1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$A - 2 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Now,

$$I_{4\times 4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_1-(A-1)C_2 \ \rightarrow \ C_1} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_2+(A-2)C_3 \to C_2} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_2-(A-1)C_4 \to C_2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{C_3 \leftrightarrow C_4} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{C_3-C_4 \to C_3} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} =: P'$$

Let P_1 be the third column of P' and let P_2 be the fourth column of P'. Then, the matrix that conjugates A to its Jordan canonical form has columns:

$$(A-I)P_1, \;\; P_1, \;\; (A-I)P_2, \;\; P_2.$$

Hence, if P is defined as

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

we have that

$$P^{-1}AP = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \; \square$$

102 Over $\mathbb{Q}$, consider the following matrix:

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

Answer the following:

(a) Prove that A is diagonalizable.

(b) Is the $\mathbb{Q}[T]$-module structure on $\mathbb{Q}^4$ by A, via $f(T) \cdot v = f(A)v$, cyclic? Explain.

Proof:

First we find the characteristic polynomial of A. Recall that

$$\chi_A(x) := \det(xI - A).$$

Calculating:

$$\begin{aligned}
\chi_A(x) &= \det(xI - A) \\
&= \det \begin{pmatrix} x & -1 & 0 & -1 \\ -1 & x & -1 & 0 \\ 0 & -1 & x & -1 \\ -1 & 0 & -1 & x \end{pmatrix} \\
&= x \cdot \det \begin{pmatrix} x & -1 & 0 \\ -1 & x & -1 \\ 0 & -1 & x \end{pmatrix} + 1 \cdot \det \begin{pmatrix} -1 & -1 & 0 \\ 0 & x & -1 \\ -1 & -1 & x \end{pmatrix} + 1 \cdot \det \begin{pmatrix} -1 & x & -1 \\ 0 & -1 & x \\ -1 & 0 & -1 \end{pmatrix} \\
&= x(x(x^2-1) + (-x)) + (-1(x^2-1) + 1(-1)) + (-1(1) - x(x) - 1(-1)) \\
&= x(x^3 - x - x) + (-x^2 + 1 - 1) + (-1 - x^2 + 1) \\
&= x^4 - 2x^2 - x^2 - x^2 \\
&= x^4 - 4x^2 \\
&= x^2(x+2)(x-2).
\end{aligned}$$

Since the minimal polynomial divides the characteristic polynomial but has all the same roots, the possibilities for the minimal polynomial are:

$$m_1(x) = x(x+2)(x-2),$$
$$m_2(x) = x^2(x+2)(x-2).$$

To figure out which is the minimal polynomial, we find the one with the least factors satisfied by A. Observe that:

$$\begin{aligned}
A(A+2I)(A-2I) &= \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} -2 & 1 & 0 & 1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -2 & 0 & 2 & 0 \\ 0 & -2 & 0 & 2 \\ 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

Therefore, the minimal polynomial of A is $x(x+2)(x-2)$ and the invariant factor list of A is:

$$x(x+2)(x-2), \quad x,$$

and elementary divisor list

$$x, \quad x, \quad x+2, \quad x-2.$$

So, the Jordan canonical form of A is

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore, A is diagonalizable. $\square$

Proof of (b):

To see that the $\mathbb{Q}[T]$-module structure is not cylic, pick

$$v := \begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix} \in \mathbb{Q}^4$$

with q_3 or q_4 nonzero. Now, note that

$$A^k = \begin{pmatrix} 2^k & 0 & 0 & 0 \\ 0 & (-2)^k & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

So, for $p(T) \in \mathbb{Q}[T]$ and $w \in V$, we have that $p(T) \cdot w = p(A)w$, which must have zeros in the third and fourth entries, and so v cannot be generated by any vector. Therefore, the $\mathbb{Q}[T]$-module structure is not cyclic. $\square$

103 Let $\mathbb{C}$ be the field of complex numbers. Prove that each irreducible $\mathbb{C}[T]$-module is isomorphic to $\mathbb{C}$.

Proof:

We need to use properties of the complex numbers, which we can just state without proof. In this case, we need that $\mathbb{C}$ is algebraically closed.

Let M be an irreducible $\mathbb{C}[T]$ module. Recall that an irreducible module is one whose only submodules are the zero module and itself. Hence, M is cyclic and generated by any nonzero element. So, $M \cong \mathbb{C}[T]/(f(T))$ for some $f(T) \in \mathbb{C}[T]$. Again by irreducibility, we have that the ideal $(f(T))$ is maximal, hence $f(T)$ is irreducible, hence $f(T)$ is linear by algebraic closure.

So, $M \cong \mathbb{C}[T]/(T - \lambda) \cong \mathbb{C}$, for some $\lambda \in \mathbb{C}$. $\square$

NOTE: This question is worded poorly. Should really say each $\mathbb{C}[T]$-module is isomorphic to $\mathbb{C}_\lambda$ for some $\lambda \in \mathbb{C}$, where $\mathbb{C}_\lambda$ is the one-dimensional vector space over $\mathbb{C}$, where T acts as multiplication by λ.

1.5 Fields

104 Prove that if F is a finite field, then there is a prime number p and a natural number n such that F has p^n elements.

Proof:

Let F be a finite field. Then, the characteristic of F is some prime p (**Fact 1**), and F has minimal subfield (i.e., prime subfield) $\mathbb{F}_p$ (**Fact 2**). Every field can be thought of as a vector space over its prime subfield (**Fact 3**). Since F is finite, it is also finite dimensional, and so we have that $F \cong \mathbb{F}_p^n$ for some integer n. Since $|\mathbb{F}_p| = p$, it follows that $|F| = |\mathbb{F}_p^n| = p^n$. □

Proof of Fact 1:

Let F be a finite field. Then, the set $\{n \cdot 1_F \mid n \in \mathbb{N}\}$ must be finite, and so there is an integer n such that $n \cdot 1_F = 0$. Let $mn \cdot 1_F = 0$. Then, since $(m \cdot 1_F)(n \cdot 1_F) = mn \cdot 1_F$, we have that if the characteristic of F is mn, then (since fields are integral domains), either $(m \cdot 1_F)$ or $(n \cdot 1_F)$ is zero, and since mn is minimal, it must be that m or n equals one, and so mn is prime. □

Proof of Fact 2:

The prime subfield of a field F is the subfield generated by 1_F. If the characteristic of F is a prime p, then the prime subfield of F is a finite field of order p, of which the only possibilty is $\mathbb{F}_p$. □

Proof of Fact 3:

Let K be a field extension over a field F. The multiplication defined in K makes K a vector space over F. It's clear that a field F is always a field extension of it's prime subfield, and so any field is a vector space over its prime subfield. □

105 Suppose that F is a subfield of K and K a subfield of L, so that the dimensions $\big[K : F\big]$ and $\big[L : K\big]$ are finite. Prove that $\big[L : F\big]$ is also finite and that

$$\big[L : F\big] = \big[L : K\big]\big[K : F\big].$$

Proof:

Define $m := \big[L : K\big]$ and $n := \big[K : F\big]$. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis for L over K and let $\{\beta_1, \ldots, \beta_n\}$ be a basis for K over F. Then, every element of L can be written as a linear combination

$$a_1\alpha_1 + \cdots + a_m\alpha_m$$

where $a_1, \ldots, a_m$ are elements of K, hence are F-linear combinations of $\beta_1, \ldots, \beta_n$:

$$a_i = b_{i,1}\beta_1 + \cdots + b_{i,n}\beta_n$$

where the $b_{i,j}$ are element of F. Substituting these expressions in for the coefficients a_i above, we see that every element of L can be written as a linear combination

$$\sum_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} b_{i,j}\alpha_i\beta_j$$

of the mn elements $\alpha_i\beta_j$ with coefficients in F. Hence, these elements span L as a vector space over F. So, $\big[L : F\big] \leq mn < \infty$.

Suppose now that we had a linear relation in L

$$\sum_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} b_{i,j}\alpha_i\beta_j = 0$$

with coefficients $b_{i,j}$ in F. Then, defining the elements $a_i \in K$ as above, this linear relation could be written

$$a_1\alpha_1 + \cdots + a_m\alpha_m = 0$$

Since the α_i are a basis for L over K, it follows that $a_1 = \cdots = a_m = 0$. Since the β_i are a basis for K over F and each $a_i = 0$, we have that

$$b_{i,1}\beta_1 + \cdots + b_{i,n}\beta_n = 0$$

and so each $b_{i,j} = 0$. Therefore, the elements $\alpha_i\beta_j$ are linearly independent, and hence form a basis for L over F of size mn. Thus,

$$\big[L : F\big] = \big[L : K\big]\big[K : F\big]. \ \square$$

106 Determine the dimension over $\mathbb{Q}$ of the extension $\mathbb{Q}\left(\sqrt{3+2\sqrt{2}}\right)$. Justify your arguments.

Proof:

Note that

$$\sqrt{3+2\sqrt{2}} = \sqrt{1+2\sqrt{2}+2} = \sqrt{(1+\sqrt{2})^2} = 1+\sqrt{2}.$$

Since $1 \in \mathbb{Q}$, we have that $\mathbb{Q}\left(\sqrt{3+2\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2}\right)$. Since $\sqrt{2} \notin \mathbb{Q}$ and $\sqrt{2}$ satisfies $x^2-2 \in \mathbb{Q}[x]$, we have that $\big[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\big] = 2$. $\square$

107 Prove that $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Conclude that $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 4$, and find a monic irreducible polynomial over $\mathbb{Q}$ satisfied by $\sqrt{3}+\sqrt{5}$.

Proof:

Clearly $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$. Observe that $(\sqrt{3}+\sqrt{5})^2 = 3+\sqrt{15}+5 = 8+2\sqrt{15}$, so $\sqrt{15} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Now, $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \ni \sqrt{15}(\sqrt{3}+\sqrt{5}) = 3\sqrt{5}+5\sqrt{3}$. Since we already have $\sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$, we can conclude

$$\frac{[3\sqrt{5}+5\sqrt{3}]-[3\sqrt{5}+3\sqrt{3}]}{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{5}),$$

and we can do the same for $\sqrt{5}$. Therefore $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$, since we showed inclusion in both directions.

To see that $\sqrt{5} \notin \mathbb{Q}\left(\sqrt{3}\right)$, assume otherwise toward a contradiction. Then, we can pick $a/b, c/d \in \mathbb{Q}$ such that

$$\sqrt{5} = \frac{a}{b} + \frac{c}{d}\sqrt{3}.$$

Now,

$$\begin{aligned}\sqrt{5}-\frac{c}{d}\sqrt{3}&=\frac{a}{b}\\ \left(\sqrt{5}-\frac{c}{d}\sqrt{3}\right)^2&=\left(\frac{a}{b}\right)^2\\ 5-2\frac{c}{d}\sqrt{15}+\frac{3c^2}{d^2}&=\frac{a^2}{b^2}\\ \frac{2c}{d}\sqrt{15}&=5+\frac{3c^2}{d^2}-\frac{a^2}{b^2}\\ \sqrt{15}&=\left(5+\frac{3c^2}{d^2}-\frac{a^2}{b^2}\right)\frac{d}{2c}\in\mathbb{Q},\end{aligned}$$

which is a contradiction.

So, it is clear that $[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2\cdot 2=4$.

To find the monic polynomial of degree 4, let $\alpha:=\sqrt{3}+\sqrt{5}$ and note that $\alpha^2=8+2\sqrt{15}$. So $2\sqrt{15}=(\alpha^2-8)$ and thus $60=(\alpha^2-8)^2$. Computing, we see that α is a solution of $x^4-16x^2+4=0$. □

108 Suppose that F is a field whose characteristic is not 2. Assume that $d_1,d_2\in F$ are not squares in F. Prove that $F\left(\sqrt{d_1},\sqrt{d_2}\right)$ is of dimension 4 over F if d_1d_2 is not a square in F and of dimension 2 otherwise.

Proof:

Note that $\left(\sqrt{d_1}+\sqrt{d_2}\right)^2=(d_1+d_2)+2\sqrt{d_1d_2}$. Hence, $\sqrt{d_1d_2}\in F\left(\sqrt{d_1}+\sqrt{d_2}\right)$.

Following the same trick as **Exercise 107**, we conclude $\sqrt{d_1},\sqrt{d_2}\in F\left(\sqrt{d_1}+\sqrt{d_2}\right)$, and hence

$$F\left(\sqrt{d_1},\sqrt{d_2}\right)=F\left(\sqrt{d_1}+\sqrt{d_2}\right).$$

If d_1d_2 is a square in F, then

$$\left(\sqrt{d_1}+\sqrt{d_2}\right)^2=(d_1+d_2)+2\sqrt{d_1d_2}\in F$$

and so

$$\left[F\left(\sqrt{d_1}+\sqrt{d_2}\right):F\right]=2.$$

Now let d_1d_2 not be a square. We must show that $\sqrt{d_2}\notin F\left(\sqrt{d_1}\right)$. Assume otherwise, and let $a,b\in F$ be such that

$$\sqrt{d_2}=a+b\sqrt{d_1}.$$

Then,

$$\begin{aligned}\sqrt{d_2}-b\sqrt{d_1}&=a\\ d_2+b^2d_1-2b\sqrt{d_1}&=a^2\\ d_2+b^2d_1-a^2&=2b\sqrt{d_2}.\end{aligned}$$

Since d_2 is not a square in F, we have that $b\neq 0$. Thus,

$$\sqrt{d_2}=\frac{1}{2b}\left(d_2+b^2d_1-a^2\right)\in F$$

which is a contradiction. Hence,

$$\left[F\left(\sqrt{d_1},\sqrt{d_2}\right):F\right]=\left[F\left(\sqrt{d_1},\sqrt{d_2}\right):F\left(\sqrt{d_1}\right)\right]\left[F\left(\sqrt{d_1}\right):F\right]=2\cdot 2=4.\ \square$$

109 Suppose that $[F(\alpha) : F]$ is odd; prove that $F(\alpha) = F(\alpha^2)$.

Proof:
Note that $\alpha^2 \in F(\alpha)$, so $F(\alpha^2)$ is an intermediate field between F and $F(\alpha)$. Note that α is a solution to the equation $x^2 - \alpha^2 \in F(\alpha^2)[x]$. Hence, $\big[F(\alpha) : F(\alpha^2)\big] \leq 2$. Recall that

$$\big[F(\alpha) : F\big] = \big[F(\alpha) : F(\alpha^2)\big]\big[F(\alpha^2) : F\big].$$

If $\big[F(\alpha) : F\big]$ is odd, then we must have that $\big[F(\alpha) : F(\alpha^2)\big] = 1$, and hence $F(\alpha) = F(\alpha^2)$. □

110 Let L be a field extension of F. Prove that the subset E of all elements of L which are algebraic over F is a subfield of L containing F.

Proof:

Note that $E = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$. It is clear that elements of F are algebraic over F, so clearly E contains F. It remains to show that E is a subfield of L.

Going back to definitions to try to find polynomials satisfying $f(\alpha + \beta) = 0$ is too tough. So, we use a theorem that says:

$$\alpha \in L \text{ is algebraic over } F \text{ if and only if } |F(\alpha) : F| \text{ is finite.}$$

Let $\alpha, \beta \in L$ be algebraic over F. Assume $\beta \neq 0$. Then, $\alpha + \beta, \alpha\beta, \alpha\beta^{-1} \in F(\alpha, \beta)$. Hence if we show that $|F(\alpha, \beta) : F| < \infty$, we'll also show that $|F(\alpha + \beta) : F|, |F(\alpha\beta) : F|, |F(\alpha\beta^{-1}) : F|$ are finite.

This is clear since $|F(\alpha) : F|$ and $|F(\beta) : F|$ are finite, and $|F(\alpha, \beta) : F| \leq |F(\alpha) : F||F(\beta) : F|$. So, we have shown that $\alpha + \beta$, $\alpha\beta$, and $\alpha\beta^{-1}$ are all algebraic. Thus, E is a subfield of L. □

111 Determine the splitting field of $x^4 - 2$ over $\mathbb{Q}$. It suffices to describe it as the subfield of $\mathbb{C}$, the field of complex numbers, generated by certain well-identified elements. Justify your choices.

Proof:

The roots in $\mathbb{C}$ of $x^4 - 2$ are:

$$\pm\sqrt[4]{2}, \quad \pm i\sqrt[4]{2}.$$

So the splitting field F of $x^4 - 2$ contains $\sqrt[4]{2}$. Since F also contains $i\sqrt[4]{2}$ and $\left(\sqrt[4]{2}\right)^{-1}$, F contains i. So, $F \subseteq \mathbb{Q}(i, \sqrt[4]{2})$. Since the roots all lie in $\mathbb{Q}(i, \sqrt[4]{2})$, we have that $F = \mathbb{Q}(i, \sqrt[4]{2})$.

Additionally, it's clear that $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 4$, since $\sqrt[4]{2}$ satisfies the polynomial $x^4 - 2$, which is irreducible by Eisenstein. Since $i \notin \mathbb{Q}\left(\sqrt[4]{2}\right)$, we have that $\left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right] = 2$. Hence,

$$\left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\right] = 4 \cdot 2 = 8. \ \square$$

112 Suppose that F is a field. For $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, define the *derivative* $D_x f(x)$ by

$$D_x[f(x)] = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

Prove the following: In a splitting field of $f(x)$, u is a multiple root of $f(x)$ if and only if u is a root of both $f(x)$ and $D_x f(x)$.

Proof:

First we prove the product rule for polynomials:
Lemma: Let $f(x)$ and $g(x)$ be polynomials in $F[x]$. Then,

$$D_x[f(x)g(x)] = D_x[f(x)] \cdot g(x) + f(x) \cdot D_x[g(x)].$$

Proof of Lemma:

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$. Recall that

$$f(x)g(x) = \sum_{i=0}^{m+n} c_i x^i,$$

where

$$c_i = \sum_{\substack{0 \le k \le n \\ 0 \le \ell \le m \\ k+\ell = i}} a_k b_\ell.$$

Now, calculating some derivatives:

$$\begin{aligned} D_x[f(x)] &= a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \\ D_x[g(x)] &= b_1 + 2b_2 x + \cdots + m b_m x^{m-1} \\ D_x[f(x)g(x)] &= \sum_{i=0}^{m+n} i c_i x^{i-1}. \end{aligned}$$

For $0 \le r < m+n$, the coefficient of x^r in $D_x[f(x)g(x)]$ is

$$(r+1)c_{r+1} = (r+1) \sum_{\substack{0 \le k \le n \\ 0 \le \ell \le m \\ k+\ell = r+1}} a_k b_\ell.$$

For $0 \le r < m+n$, the coefficient of x^r in $D_x[f(x)]g(x)$ is

$$\sum_{\substack{0 \le k \le n-1 \\ 0 \le \ell \le m \\ k+\ell = r}} (k+1) a_{k+1} b_\ell.$$

For $0 \le r < m+n$, the coefficient of x^r in $f(x)D_x[g(x)]$ is

$$\sum_{\substack{0 \le k \le n \\ 0 \le \ell \le m-1 \\ k+\ell = r}} (\ell+1) a_k b_{\ell+1}.$$

Therefore, for $0 \le r < m+n$, the coefficient of x^r in $D_x[f(x)] \cdot g(x) + f(x) \cdot D_x[g(x)]$ is

$$\sum_{\substack{0 \le k \le n-1 \\ 0 \le \ell \le m \\ k+\ell = r}} (k+1) a_{k+1} b_\ell + \sum_{\substack{0 \le k \le n \\ 0 \le \ell \le m-1 \\ k+\ell = r}} (\ell+1) a_k b_{\ell+1} = (r+1) \sum_{\substack{0 \le k \le n \\ 0 \le \ell \le m \\ k+\ell = r+1}} a_k b_\ell = (r+1)c_{r+1}.$$

Hence, the coefficient of each power of x is the same, and so

$$D_x[f(x)g(x)] = D_x[f(x)] \cdot g(x) + f(x) \cdot D_x[g(x)]. \ \square$$

($\Longleftarrow$) :

Let u be a multiple root of $f(x)$. Then, $f(x) = (x-u)^\alpha g(x)$, where $\alpha \geq 2$ is an integer and $g(x)$ is a polynomial. By the above product rule for polynomials:

$$\begin{aligned} D_x[f(x)] &= D_x[(x-u)^\alpha g(x)] \\ &= \alpha(x-u)^{\alpha-1} \cdot g(x) + (x-u)^\alpha \cdot D_x[g(x)] \\ &= (x-u)\left[\alpha(x-u)^{\alpha-2} \cdot g(x) + (x-u)^{\alpha-1} \cdot D_x[g(x)]\right], \end{aligned}$$

where $\alpha - 2 \geq 0$. Hence, u is a root of $D_x[f(x)g(x)]$. $\square$

($\Longrightarrow$) :

Let $(x-u)$ be a factor of $f(x)$ and $D_x[f(x)]$. So, $f(x) = (x-u) \cdot g(x)$ for some polynomial $g(x)$. Then, by the above product rule for polynomials:

$$\begin{aligned} D_x[f(x)] &= D_x[(x-u) \cdot g(x)] \\ &= g(x) + (x-u) \cdot D_x[g(x)]. \end{aligned}$$

Since $D_x[f(x)]$ has a factor of $(x-u)$ be assumption, we must have that $g(x)$ has a factor of $(x-u)$. Therefore, $f(x)$ has at least two factors of $(x-u)$ and so u is a multiple root of $f(x)$. $\square$

113 Assume the existence and uniqueness, up to isomorphism, of the splitting of a polynomial over an arbitrary base field. Let p be a prime number. Now consider the polynomial $x^{p^n} - x$ over the field $\mathbb{F}_p$ of p elements. Let K_{p^n} be its splitting field. Prove that K_{p^n} has p^n elements. Now consider any field $\mathbb{F}$ having p^n elements and prove that $\mathbb{F} \cong K_{p^n}$.

Proof:

Consider the polynomial $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$. The derivative of this polynomial is $p^n x^{p_n - 1} - 1$. Since $\mathbb{F}_p$ has characteristic p, this polynomial equals -1, which has no roots. Therefore, the polynomial $x^{p^n} - x$ has no multiple roots, so must have p^n distinct roots.

Let α and β be roots of $f(x)$, so that $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Now, since $\mathbb{F}_p$ has characteristic p, we have that

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

and additionally

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta.$$

Therefore, $\alpha + \beta$ and $\alpha\beta$ are also roots of $f(x)$.

So, the roots of $f(x)$ form a field K_{p^n} that contains exactly p^n elements, and in fact K_{p^n} is the splitting field of the polynomial $f(x)$. Since $\mathbb{F}_p$ is a subfield of K_{p^n}, we have that K_{p^n} is a field extension over $\mathbb{F}_p$, with $\left[K_{p^n} : \mathbb{F}_p\right] = n$. Hence, we have shown the existence of fields with p^n elements.

To see uniqueness, let $\mathbb{F}$ be a field with characteristic p and p^n elements. Note that the multiplicative group $\mathbb{F}^\times$ has order $p^n - 1$, and so $\alpha^{p^n - 1} = 1$ for every nonzero $\alpha \in \mathbb{F}$. Hence, for every nonzero $\alpha \in F$ we have that $\alpha^{p^n} = \alpha$, i.e., α is a root of the polynomial $x^{p^n} - x$. So,

$\mathbb{F}$ is the splitting field of this polynomial and since all splitting fields of a given polynomial are isomorphism, we conclude that $\mathbb{F} \cong K_{p^n}$. $\square$

Chapter 2

Important Theorems

2.1 Groups

Theorem: (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\dfrac{|G|}{|H|}$.

Proof:

Let $|H| = n$ and let the number of left cosets of H in G equal k. Recall that the set of left cosets of H in G partitions G. By the definition of a left coset, the map

$$H \to gH \quad \text{defined by} \quad h \mapsto gh$$

is a surjection from H to the left coset gH. The left cancellation law implies that this map is injective since $gh_1 = gh_2$ implies $h_1 = h_2$. This proves that H and gH have the same order:

$$|gH| = |H| = n.$$

Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Thus,

$$k = \frac{|G|}{n} = \frac{|G|}{|H|}. \ \square$$

Theorem:

If H and K are finite subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof:

Notice that HK (which is not necessarily a subgroup) is a union of left cosets of K, namely,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of *distinct* left cosets of the form hK, for $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK, for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by **Lagrange's Theorem**, equals $\dfrac{|H|}{|H \cap K|}$. Thus HK consists of $\dfrac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has $|K|$ elements) which gives the formula above. $\square$

Theorem: (First Isomorphism Theorem)

If $\varphi : G \to H$ is a homomorphism of groups, then $\operatorname{Ker}(\varphi) \trianglelefteq G$ and $G/\operatorname{Ker}(\varphi) \cong \varphi(G)$.

Proof:

First we prove that $\operatorname{Ker}(\varphi) \trianglelefteq G$. Let $k \in \operatorname{Ker}(\varphi)$ and $g \in G$. Then,

$$\begin{aligned}\varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g^{-1}) \\ &= \varphi(g)\varphi(k)\varphi(g)^{-1} \\ &= \varphi(g)1_H\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= 1_H.\end{aligned}$$

Hence $gkg^{-1} \in \operatorname{Ker}(\varphi)$ and so $\operatorname{Ker}(\varphi) \trianglelefteq G$.

Now define the map $\theta : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ such that $gK \mapsto \varphi(g)$. First we show that θ is well-defined. Let g_1 and g_2 be elements of the same coset, so that $g_1 \operatorname{Ker}(\varphi) = g_2 \operatorname{Ker}(\varphi)$ and $g_1^{-1}g_2 \in \operatorname{Ker}(\varphi)$. So, $\varphi(g_1^{-1}g_2) = 1$ and hence $\varphi(g_1) = \varphi(g_2)$. Thus, θ is well-defined.

Next we verify that θ is a homomorphism. Let $g_1 \operatorname{Ker}(\varphi)$ and $g_2 \operatorname{Ker}(\varphi)$ be two cosets of $\operatorname{Ker}(\varphi)$.

$$\begin{aligned}\theta(g_1 \operatorname{Ker}(\varphi) \cdot g_2 \operatorname{Ker}(\varphi)) &= \theta(g_1g_2 \operatorname{Ker}(\varphi)) \\ &= \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= \theta(g_1 \operatorname{Ker}(\varphi))\theta(g_2 \operatorname{Ker}(\varphi)).\end{aligned}$$

Hence θ is a homomorphism.

Lastly we show that θ is a bijection. The kernel of θ is all cosets $g \operatorname{Ker}(\varphi)$ such that $\varphi(g) = 1$. The only such coset is the identity coset $1_H \operatorname{Ker}(\varphi)$. Therefore since the kernel of θ is trivial, we have that θ is injective. If $h \in \operatorname{Im}(\varphi)$, then $h = \varphi(g)$ for some $g \in G$. Now, $\theta(gK) = \varphi(g) = h$. So, θ is surjective. Hence, θ is a bijective homomorphism, i.e. and isomorphism, and so we have that $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$. $\square$

Theorem: (Second / Diamond Isomorphism Theorem)

Let G be a group, let A and B be subgroups of G and assume that $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A/A \cap B$.

Proof:

Recall that $A \leq N_G(B)$ implies that AB is a subgroup of G. Additionally, since $A \leq N_G(B)$ (by assumption) and $B \leq N_G(B)$ (trivially), we have that $AB \leq N_G(B)$, i.e., $B \trianglelefteq AB$. Since $B \trianglelefteq AB$, the quotient group AB/B is well defined. Consider the map $\varphi : A \to AB/B$ defined by $\varphi(a) = aB$. It is clear that φ is a homomorphism, as it is just the restriction to the subgroup A of the natural projection homomorphism $\pi : AB \to AB/B$. It is also clear that φ is surjective and that there kernel of φ is $A \cap B$. By the **First Isomorphism Theorem**, $A \cap B \trianglelefteq A$ and $A/A \cap B \cong AB/B$. $\square$

Theorem: (Third Isomorphism Theorem)

Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then, $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

Proof:

First we show that $K/H \trianglelefteq G/H$. Let $kH \in K/H$ and $gH \in G/H$. Note that $(gH)(kH)(gH)^{-1} = (gkg^{-1})H$. Since $K \trianglelefteq G$, we have that $gkg^{-1} \in K$, and so $gkg^{-1}H \in K/H$. Therefore, $K/H \trianglelefteq G/H$.

Now consider the map $\varphi : G/H \to G/K$ defined by $\varphi(gH) = gK$. Assume that $g_1H = g_2H$, so that $g_1g_2^{-1} \in H \leq K$. Because $g_1g_2^{-1} \in K$, we have that $g_1K = g_2K$, i.e., $\varphi(g_1H) = \varphi(g_2H)$, and so φ is well defined. It is clear that φ is surjective because for any $gK \in G/K$, the cost $gH \in G/H$ maps to gK. Lastly, φ is a homomorphism because

$$\begin{aligned}\varphi(g_1H \cdot g_2H) &= \varphi(g_1g_2H)\\ &= g_1g_2K\\ &= g_1K \cdot g_2K\\ &= \varphi(g_1H)\varphi(g_2H).\end{aligned}$$

Next, observe that

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{gH \in G/H \mid \varphi(gH) = 1K\}\\ &= \{gH \in G/H \mid gK = 1K\}\\ &= \{gH \in G/H \mid g \in K\}\\ &= K/H.\end{aligned}$$

Therefore, by the **First Isomorphism Theorem of Groups**, we have that

$$(G/H)/(K/H) \cong G/K. \ \square$$

Theorem: (Fourth / Lattice Isomorphism Theorem)

Let G be a group and let $N \trianglelefteq G$. Then, there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

(2) if $A \leq B$, then $\big[B : A\big] = \big[\overline{B} : \overline{A}\big]$,

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

Proof:

First we show that there is a bijection between the subgroups of G containing N and the subgroups of A/N. Let φ be the map $A \mapsto A/N$, where A is a subgroup of G containing N. Let $A/N = B/N$. Then, for all $a \in A$, there exists $b \in B$ such that $aN = bN$, i.e., $b^{-1}a \in N \subseteq B$. If $b^{-1}a \in B$, then it's clear that $a \in B$, and so $A \subseteq B$. By a symmetrical argument, $B \subseteq A$, and thus $A = B$. Therefore, φ is injective. Now let S be a subgroup of G/N. Each element of

S is of the form gN for $g \in G$. Let T be the set of all element $h \in G$ such that $hN \in S$. As sets, it's clear that $N \subseteq T$, and it remains to show that the set T is in fact a subgroup of G. If g_1 and g_2 are elements of T such that $g_1N \in S$ and $g_2N \in S$, then since S is a subgroup, $(g_1N)(g_2N)^{-1} = g_1g_2^{-1}N \in S$, and so $g_1g_2^{-1} \in T$. So, we have shown that for every subgroup S of G/N, there exists a subgroup T of G containing N such that $\varphi(T) = S$, i.e., φ is surjective. Hence, φ is a bijection, which completes the first part of the proof, and we now have the fact that every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N.

We now prove the five properties.

(1) Let $A \leq B$. Then it is trivial that $A/N \leq B/N$ because if $aN \in A/N$, then $a \in A$, so $a \in B$, hence $aN \in B/N$.

Let $A/N \leq B/N$. If $a \in A$, then $aN \in B/N$, i.e., $b^{-1}a \in N \subseteq B$ for some $b \in B$. Thus, $a \in B$. So, $A \leq B$.

(2) We will show that $|B/A| = |(B/N)/(A/N)|$ and the theorem will follow. Note that we cannot use the **Third Isomorphism Theorem**, since we do not have that $A \trianglelefteq B$. We can still consider the cosets, however. Let $\psi : B/A \to (B/N)/(A/N)$ be defined by $\psi(bA) = (bN)(A/N)$. First we show that ψ is well defined and injective:

$$\begin{aligned} b_1A = b_2A &\iff b_1^{-1}b_2 \in A \\ &\iff (b_1N)^{-1}(b_2N) = b_1^{-1}b_2N \in A/N \\ &\iff (b_1N)(A/N) = (b_2N)(A/N). \end{aligned}$$

Additionally, it is clear that ψ is surjective since for any $(bN)(A/N)$ we can pick bA from B/A and then $\psi(bA) = (bN)(A/N)$. Hence, ψ is a bijection, and so $|B/A| = |(B/N)/(A/N)|$, and the theorem follows.

(3) Let $x \in \langle A, B\rangle/N$. Then, $x = yN$, where $y = c_1c_2 \cdots c_k$ for $c_i \in A \cup B$. So,

$$\begin{aligned} x &= yN \\ &= (c_1c_2 \cdots c_k)N \\ &= (c_1N)(c_2N) \cdots (c_kN) \\ &\in \langle A/N, B/N\rangle. \end{aligned}$$

Similarly, if $xN \in \langle A/N, B/N\rangle$, then $xN = (c_1N)(c_2N) \cdots (c_kN)$, where $c_iN \in A/N \cup B/N$. Now,

$$\begin{aligned} xN &= (c_1N)(c_2N) \cdots (c_kN) \\ &= (c_1c_2 \cdots c_k)N \\ &\in \langle A, B\rangle/N. \end{aligned}$$

(4) Let $xN \in (A \cap B)/N$. Then, $xN = yN$ for some $y \in A \cap B$, and since $N \subseteq A \cap B$, we have that $x \in A \cap B$. Therefore, $xN \in A/N$ and $xN \in B/N$, and so $xN \in (A/N \cap B/N)$.

Let $xN \in (A/N \cap B/N)$. Then, $xN = yN$ for some $y \in A$, and since $N \subseteq A$, we have $x \in A$. Similarly, $x \in B$. Therefore, $x \in (A \cap B)$ and so $xN \in (A \cap B)/N$.

(5) Let $A \trianglelefteq G$. Then, let $aN \in A/N$ and $gN \in G/N$. Consider

$$\begin{aligned} (gN)(aN)(gN)^{-1} &= (gN)(aN)(g^{-1}N) \\ &= (gag^{-1})N \\ &= a_1N \\ &\in A/N, \end{aligned}$$

with $a_1 \in A$ since $A \trianglelefteq G$. Therefore, $A/N \trianglelefteq G/N$.

Conversely, let $A/N \trianglelefteq G/N$ and let $a \in A$ and $g \in G$. Consider the coset $(gag^{-1})N = (gN)(aN)(gN)^{-1} \in A/N$ by normality. So, $gag^{-1}N = a_1N$ for some $a_1 \in A$. Hence, $a_1^{-1}gag^{-1} \in N \subseteq A$ and thus $gag^{-1} \in A$, and so $A \trianglelefteq G$.

The proof is now complete. □

Theorem: (Class Equation)

Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \big[G : C_G(g_1)\big].$$

Proof:

Recall that each element in the center of G is its own singleton conjugacy classes, denote $\{1\}, \{z_2\}, \ldots, \{z_m\}$. Let $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_r$ be the conjugacy classes of G not contained in the center, and let g_i be the representative for $\mathcal{K}_i$. Then, the full set of conjugacy classes of G is given by

$$\{1\}, \{z_2\}, \ldots, \{z_m\}, \mathcal{K}_1, \ldots, \mathcal{K}_r.$$

Since the conjugacy classes completely partition G, we have that

$$\begin{aligned} |G| &= \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |\mathcal{K}_i| \\ &= |Z(G)| + \sum_{i=1}^{r} \big[G : C_G(g_i)\big]. \end{aligned}$$

The fact that $|\mathcal{K}_i| = \big[G : C_G(g_i)\big]$ comes from the **Orbit Stabilizer Theorem**, applied to the action on conjugation. □

Theorem: (Cauchy's Theorem)

If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof:

We proceed by induction on $n = |G|$ and consider two separate cases: G is abelian or G is nonabelian.

Let G be abelian. If G is simple, then it must be cyclic of prime order, and so $|G| = p$, i.e. every nontrivial element has order p. If G is not simple, then it has some nontrivial proper normal subgroup $H \trianglelefteq G$. If $p \mid |H|$ then by the induction hypothesis, H has an element of order p and hence so does G. If $p \nmid |H|$, then $p \mid \big[G : H\big]$, and so G/H has an element of order p again by the induction hypothesis. So, there exists $x \in G$ such that $(xH)^p = x^pH = H$. So, $\langle x^p \rangle < \langle x \rangle$, i.e. $|x^p| < |x|$. Thus, $p \mid |x|$ and so if we write $|x| = pk$, we have that x^k is an element of order p. This completes the abelian case.

Now let G be nonabelian, so that $Z(G) < G$. If $p \mid |C_G(a)|$ for some $a \notin Z(G)$, then $C_G(a)$ is a proper subgroup and by the induction hypothesis has an element of order p, which must also be an element of order p in G. Otherwise, $p \mid \big[G : C_G(a)\big]$ for all $a \notin Z(G)$, so by the class equation we have that $p \mid |Z(G)|$. By the induction hypothesis, $Z(G)$, and hence G, contains an element of order p. □

Theorem: (Jordan-Hölder Theorem)

Let G be a finite group with $G \neq 1$. Then

(1) G has a composition series, and

(2) The composition factors in a composition series are unique, up to a permutation.

Proof:

We prove the existence of the composition series by induction on $n = |G|$. If $n = 1$ or if G is simple, the result holds. Otherwise, pick a maximal proper normal subgroup N of G. By the induction hypothesis, the group N has some composition series of length k. By adding G as the last term, G now has a composition series of length $k + 1$, since G/N must be simple. So, existence is proven.

To prove uniqueness, we proceed by induction on the length n of the decomposition series. If $n = 1$, then G is simple and we are done. If $n > 1$, then suppose that we have two composition series for G:

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G,$$

$$1 = M_0 \leq M_1 \leq \cdots \leq M_s = G.$$

If $N_{r-1} = M_{s-1}$, then we can apply the induction hypothesis and we're done. Otherwise, assume $N_{r-1} \neq M_{s-1}$. Define $H = N_{r-1} \cap M_{s-1}$ and choose for it a decomposition series

$$1 = H_0 \leq H_1 \leq \cdots \leq H_k = H.$$

By the **Second Isomorphism Theorem** and the fact that $N_{r-1} < N_{r-1}M_{s-1} \trianglelefteq G$,

$$N_{r-1}/H = N_{r-1}M_{s-1}/M_{s-1} = G/M_{s-1}$$

In particular, $H \trianglelefteq N_{r-1}$ and their quotient is simple. Thus,

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{r-2} \leq N_{r-1}, \text{ and}$$

$$1 = H_0 \leq H_1 \leq \cdots \leq H_k \leq N_{r-1}$$

are two decomposition series for N_{r-1}. By the induction hypothesis, they have the same simple quotients. A similar result holds for the M_{s-1} series, and hence $s = r$. Moreover, since $G/N_{r-1} = M_{s-1}/H$ and $G/M_{s-1} = N_{r-1}/H$ (by the **Second Isomorphism Theorem** again), we have now accounted for all of the simple quotients, and shown that they are the same. □

Theorem:

Let $N \trianglelefteq G$. If N and G/N are solvable, then G is solvable.

Proof:

Let $\overline{G} := G/N$ and similarly use the bar notation to denote reduction modulo N. Let $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$ be a chain of subgroups of N such that N_{i+1}/N_i is abelian for all i. Let $\overline{1} = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \cdots \trianglelefteq \overline{G_m} = \overline{G}$ be a chain of subgroups of $\overline{G}$ such that $\overline{G_{i+1}}/\overline{G_i}$ is abelian.

By the **Fourth (Lattice) Isomorphism Theorem**, there exist subgroups G_i of G with $N \leq G_i$ such that $G_i/N = \overline{G_i}$ and it holds that $G_i \trianglelefteq G_{i+1}$. By the **Third Isomorphism Theorem**

$$\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i.$$

Hence, there exists the following chain of subgroups of G:

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

which has the property that successive quotients are abelian. Therefore, G is solvable. $\square$

Theorem: (Cayley's Theorem)

Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.

Proof: See **First Year Pool, Exercise 1**.

Theorem:

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Proof:

Suppose $H \leq G$ and $\big[G : H\big] = p$. Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G. Let $K := \mathrm{Ker}(\pi_H)$ and let $k := \big[H : K\big]$. Then, $\big[G : K\big] = \big[G : H\big]\big[H : K\big] = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p (namely, the image of G under π_H) by the **First Isomorphism Theorem**. By **Lagrange's Theorem**, $pk = |G/K| \mid p!$. Thus $k \mid \dfrac{p!}{p} = (p-1)!$. But, all prime divisors of $(p-1)!$ are less than p and by the minimality of p, every prime divisor of k is greater than or equal to p. This forces $k = 1$, so that $H = K \trianglelefteq G$. $\square$

Theorem:

A_5 is simple.

Proof: See **First Year Pool, Exercise 35**.

Theorem: (Conjugation is an Automorphism)

Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \qquad \text{for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Proof:

Let φ_g be conjugation by g. Note that because g normalizes H, φ_g maps H to itself. Since we have already seen that conjugation defines an action, it follows that $\varphi_1 = 1$ (the identity map on G) and $\varphi_a \circ \varphi_b = \varphi_{ab}$ for all $a, b \in G$. Thus each φ_g gives a bijection from H to itself since it has a 2-sided inverse $\varphi_{g^{-1}}$. Each φ_g is a homomorphism from H to H because

$$\varphi_g(hk) = g(hk)g^{-1} = gh(gg^{-1})kg^{-1} = (ghg^{-1})(gkg^{-1}) = \varphi_g(h)\varphi_g(k)$$

for all $h, k \in H$. This proves that conjugation by any fixed element of G defines an automorphism of H.

By the preceding remark, the permutation representation $\psi : G \to S_H$ defined by $\psi(g) = \varphi_g$ (which we have already proved is a homomorphism) has image contained in the subgroup $\mathrm{Aut}(H)$

of S_H. Finally,

$$\begin{aligned}\mathrm{Ker}(\psi) &= \{g \in G \mid \varphi_g = \mathrm{Id}\} \\ &= \{g \in G \mid ghg^{-1} = h \text{ for all } h \in G\} \\ &= C_G(H).\end{aligned}$$

The **First Isomorphism Theorem** implies the final statement of the proposition. □

Corollary: (N/C Theorem) For any subgroup H of G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Proof: Since $H \trianglelefteq N_G(H)$, we apply the theorem to $N_G(H)$. In the second case, we use $H = G$ which yields $N_G(G) = G$ and $C_G(G) = Z(G)$.

Theorem: (Sylow's Theorem)

Let G be a group of order $p^\alpha m$ where p is a prime not dividing m.

(1) Sylow p-subgroups of G exists, i.e., $\mathrm{Syl}_p(G) \neq \emptyset$.

(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.

(3) The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \pmod{p}.$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Lemma:

Let $P \in \mathrm{Syl}_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Proof of Lemma:

Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$ it is clear that $P \cap Q \leq H$, so we must prove the reverse inclusion. Since by definition $H \leq Q$, this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p-subgroup of G containing both P and H; but P is a p-subgroup of G of largest possible order, so we must have $PH = P$, i.e. $H \leq P$.

Since $H \leq N_G(P)$, we have that PH is a subgroup of G. Additionally,

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

All the numbers in the above quotient are powers of p, and so PH is a p-group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^α, the largest power of p which divides $|G|$. These two facts force $|PH| = p^\alpha = |P|$. This in turn implies $P = PH$ and $H \leq P$. This establishes the lemma. □

Proof of Theorem:

Part (1): We proceed by induction on $|G|$. If $|G| = 1$, there is nothing to prove. Assume the existence of Sylow p-subgroups for all groups of order less than $|G|$.

If p divides $|Z(G)|$, then by Cauchy's Theorem, $Z(G)$ has a subgroup N of order p. Let $\overline{G} = G/N$ so that $|\overline{G}| = p^{\alpha-1}m$. By induction, $\overline{G}$ has a subgroup $\overline{P}$ of order $p^{\alpha-1}$. Let P be the subgroup of G containing N such that $\overline{P} = P/N$. Then

$$|P| = |P/N| \cdot |N| = p^{\alpha-1} \cdot p = p^{\alpha}.$$

Then P is a Sylow p-subgroup of G.

Now consider the case where p does not divide $Z(G)$. Let $g_1, \ldots, g_r$ be representatives of the distinct non-central conjugacy classes of G. The class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} \big[G : C_G(g_i)\big].$$

If $p \mid \big[G : C_G(g_i)\big]$ for all i, then we would have $p \mid |Z(G)|$, which is a contradiction, thus there exists i with p not dividing $\big[G : C_G(g_i)\big]$. Let $H = C_G(g_i)$ for this i so that $|H| = p^{\alpha}k$, where $p \nmid k$. Since $g_i \notin Z(G)$, $|H| < |G|$. By induction, H has a Sylow p-subgroup P which is a subgroup of G. Since $|P| = p^{\alpha}$, P is a Sylow p-subgroup of G. This completes the induction and proves (1).

Before proving (2) and (3), we make some calculations. By (1) there exists a Sylow p-subgroup P of G. Let

$$\mathcal{S} := \{P_1, P_2, \ldots, P_r\}$$

be the set of all conjugates of P (i.e., $\mathcal{S} = \{gPg^{-1} \mid g \in G\}$) and let Q be *any* p-subgroup of G. By the definition of $\mathcal{S}$, G and hence also Q acts by conjugation on S. Write $\mathcal{S}$ as a disjoint union of orbits under this action by Q:

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s$$

where $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$. Keep in mind that r does not depend on Q but the number of Q-orbits s does (note that by definition, G has only one orbit on $\mathcal{S}$ but a subgroup Q of G may have more than one orbit). Renumber the elements of $\mathcal{S}$ if necessary so that the first s elements of $\mathcal{S}$ are representatives of the Q-orbits: $P_i \in \mathcal{O}_i$, $1 \le i \le s$. By the **Orbit-Stabilizer Theorem**, we have that $|\mathcal{O}_i| = \big[Q : N_Q(P_i)\big]$. By definition, $N_Q(P_i) = N_G(P_i) \cup Q$. By the **Lemma**, $N_G(P_i) \cap Q = P_i \cap Q$. Combining these two facts gives

$$|\mathcal{O}_i| = \big[Q : P_i \cap Q\big], \quad 1 \le i \le s.$$

We are now in a position to prove that $r \equiv 1 \pmod{p}$; Since Q was arbitrary, we may take $Q = P_1$ above, so that part (1) gives

$$|\mathcal{O}_1| = 1.$$

Now, for all $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$. By (1),

$$|\mathcal{O}_i| = \big[P_1 : P_1 \cap P_i\big] > 1, \quad 2 \le i \le s.$$

Since P_1 is a p-group, $\big[P_1 : P_1 \cap P_i\big]$ must be a power of p, so that

$$p \mid |\mathcal{O}_i|, \quad 2 \le i \le s.$$

Thus

$$r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|) \equiv 1 \pmod{p}.$$

We now prove parts (2) and (3). Let Q be any p-subgroup of G. Suppose Q is not contained in P_i for any $i \in \{1, 2, \ldots, r\}$ (i.e., $Q \not\leq gPg^{-1}$ for any $g \in G$). In this situation, $Q \cap P_i < Q$ for all i, so by (1)

$$|\mathcal{O}_i| = \big[Q : Q \cap P_i\big] > 1, \quad 1 \le i \le s.$$

Thus, $p \mid |\mathcal{O}_i|$ for all i, so p divides $|\mathcal{O}_1| + \cdots + |\mathcal{O}_s| = r$. This contradicts the fact that $r \equiv 1 \pmod{p}$ (remember, r does not depend on the choice of Q). This contradiction proves $Q \leq gPg^{-1}$ for some $g \in G$.

To see that all Sylow p-subgroups of G are conjugate, let Q be any Sylow p-subgroup of G. By the preceding argument, $Q \leq gPg^{-1}$ for some $g \in G$. Since $|gPg^{-1}| = |Q| = p^\alpha$, we must have $gPg^{-1} = Q$. This establishes part (2). In particular $\mathcal{S} = \mathrm{Syl}_p(G)$, since *every* Sylow p-subgroup of G is conjugate to P, and so $n_p = r \equiv 1 \pmod{p}$, which is the first part of (3).

Finally, since all Sylow p-subgroups are conjugate, the **Orbit-Stabilizer Theorem** tells us that

$$n_p = \big[G : N_G(P)\big] \quad \text{for any } P \in \mathrm{Syl}_p(G),$$

completing the proof of Sylow's Theorem. □

Theorem:

Let $P \in \mathrm{Syl}_p(G)$. Then, the following are equivalent:

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$.

(2) P is normal in G.

(3) P is characteristic in G.

(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Proof:

Assume (1) holds. Then, $gPg^{-1} = P$ for all $g \in G$ since $gPg^{-1} \in \mathrm{Syl}_p(G)$. Hence, $P \trianglelefteq G$. Conversely, assume (2) holds and $Q \in \mathrm{Syl}_p(G)$. Then, there exists $g \in G$ such that $Q = gPg^{-1} = P$, and so P is the unique Sylow p-subgroup.

Assume (2) holds. Since P must be the unique Sylow p-subgroup by the above argument, every automorphism must map P to P. Hence P is characteristic in G. Conversely, assume (3) holds. Since characteristic subgroups are normal, (2) holds.

Assume (1) holds and let X be a subset of G such that $|x|$ is a power of p for all $x \in X$. By the conjugacy part of **Sylow's Theorem**, for each $x \in X$, there is some $g \in G$ such that $x \in gPg^{-1} = P$. Thus, $X \subseteq P$ and so $\langle X \rangle \leq P$, and this means $\langle X \rangle$ must be a p-group. Conversely, if (4) holds, let X be the union of all Sylow p-subgroups of G. If P is any Sylow p-subgroup, P is a subgroup of the p-group $\langle X \rangle$. Since P is a p-subgroup of G of maximal order, we must have $P = \langle X \rangle$, so (1) holds. □

Theorem: (Recognition Theorem)

Suppose G is a group with subgroups H and K such that

(1) H and K are normal in G, and

(2) $H \cap K = 1$.

Then, $HK \cong H \times K$.

Proof:

Observe that by hypothesis (1), HK is a subgroup of G. Let $h \in H$ and let $k \in K$. Since $H \trianglelefteq G$, we have that $k^{-1}hk \in H$, so that $h^{-1}(k^{-1}hk) \in H$. Similarly, $(h^{-1}k^{-1}h)k \in K$. Since $H \cap K = 1$, we have that $hk = kh$ and so every element of H commutes with every element of K.

Since $H \cap K = 1$, each element of HK can be written uniquely as a product hk, with $h \in H$ and $k \in K$. Thus, the map $\varphi : HK \to H \times K$, defined by $hk \mapsto (h, k)$ is well-defined. To see that φ is a homomorphism, note that if $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then we have seen that h_2 and k_1 commute. Hence $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$, and the latter product is the unique way of writing $(h_1k_1)(h_2k_2)$ in the form hk with $h \in H$ and $k \in K$. This shows that

$$\begin{aligned}\varphi(h_1k_1h_2k_2) &= \varphi(h_1h_2k_1k_2)\\ &= (h_1h_2, k_1k_2)\\ &= (h_1, k_1)(h_2, k_2)\\ &= \varphi(h_1k_1)\varphi(h_2k_2)\end{aligned}$$

so that φ is a homomorphism. The homomorphism φ is a bijection since the representation of each element of HK as a product of the form hk is unique, which proves that φ is an isomorphism. □

2.2 Rings

Theorem:

Any finite integral domain is a field.

Proof:

Let R be a finite integral domain and let a be a nonzero element of R. By the cancellation law the map $x \mapsto ax$ is an injective function. Since R is finite this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e, a is a unit in R. Since a was an arbitrary nonzero element, R is a field. □

Theorem:

In a ring with identity, every proper ideal is contained in a maximal ideal.

Proof: See **First Year Pool, Exercise 49**.

Theorem:

Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof:

The ideal M is maximal if and only if there are no ideals I with $M \subset I \subset R$. By the **Fourth (Lattice) Isomorphism Theorem**, the ideals of R containing M correspond bijectively with the ideals of R/M, so M is maximal if and only if the only ideals of R/M are 0 and R/M. This is case if and only if R/M is a field. □

Theorem:

Assume R is commutative. Then, the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof:

This proof is simply a matter of translating the definition of a prime ideal into the language of quotients. The ideal P its prime if and only if $P \neq R$ and whenever $ab \in P$ then either $a \in P$ or $b \in P$. Use the bar notation for elements of R/P: $\overline{r} = r + P$. Note that $r \in P$ if and only if $\overline{r}$ is zero in the quotient ring R/P. Thus, in the terminology of quotients, P is a prime ideal if and only if $\overline{R} \neq \overline{0}$ and whenever $\overline{ab} = \overline{a}\overline{b} = 0$, then either $\overline{a} = 0$ or $\overline{b} = 0$, i.e., R/P is an integral domain. □

Since fields are integral domains, it is a direct corollary that all maximal ideals are prime ideals.

Theorem: (Every Euclidean Domain is a Principal Ideal Domain)

Proof:

Let R be a Euclidean Domain. Let I be an ideal of R. If I is the zero ideal, then $I = (0)$ and the theorem holds. Otherwise, let d be a nonzero element of minimum norm (such a d exists since the set $\{N(a) \mid a \in I\}$ has a minimal element by the Well Ordering of $\mathbb{Z}$). It is clear that $(d) \subseteq I$ since $d \in I$. To see the reverse inclusion, let $a \in I$. By the Division Algorithm, we can write $a = qd + r$ for some $q, r \in R$ with $r = 0$ or $N(r) < N(d)$. Since d has minimal norm, we must have $r = 0$. Hence, $a = qd \in (d)$. Since we've shown inclusion in both directions, we have shown that $I = (d)$. □

Theorem:

Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof:

Let (p) be a nonzero prime ideal in the Principal Ideal Domain R and let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now, $p \in (m)$ and so $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p). If $m \in (p)$ then $(p) = (m) = I$. If, on the other hand, $r \in (p)$, write $r = ps$. In this case, $p = rm = psm$, and so $sm = 1$ (here we use the fact that R is an integral domain to do the cancellation) and m is a unit, so $I = R$. □

Theorem:

In an integral domain, a prime element is always irreducible.

Proof:

Suppose (p) is a nonzero prime ideal and $p = ab$. Then, $ab = p \in (p)$, so by definition of prime ideal, one of a or b, say a, is in (p). Thus $a = pr$ for some r. This implies $p = ab = prb$ so $rb = 1$ and b is a unit. This shows that p is irreducible. □

Theorem:

In a Principal Ideal Domain, a nonzero element is a prime if and only if it is irreducible.

Proof:

By the above theorem, it remains to show that if p is irreducible, then p is prime, i.e., (p) is a prime ideal. If M is any ideal containing (p) then by hypothesis $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = rm$ for some r. But p is irreducible so by definition either r or m is a unit. This means that either $(p) = (m)$ or $(m) = (1)$, respectively. Thus, the only ideals containing (p) are (p) or (1), i.e., (p) is maximal ideal. Since nonzero prime ideals in a Principal Ideal Domain are maximal ideals, p is prime. □

Theorem:

Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I. Then, $R[x]/(I) \cong (R/I)[x]$.

In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Proof:

There is a natural map $\varphi : R[x] \to (R/I)[x]$ given by reducing each of the coefficients of a polynomial modulo I. The definition of addition and multiplication in these two rings shows that φ is a ring homomorphism. The kernel is precisely the set of polynomials each of whose coefficients is an element of I, which is to say that $\mathrm{Ker}(\varphi) = I[x] = (I)$, proving the first part. The last statement follows from the fact that if a ring S is an integral domain then the ring $S[x]$ also is. If I is a prime ideal of R, then R/I is an integral domain, and thus so is $(R/I)[x]$. Therefore, by the isomorphism, (I) is a prime ideal. □

Theorem: (Gauss' Lemma)

Let R be a Unique Factorization domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements, $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Proof:

The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the Unique Factorization Domain R. Multiplying through by a common denominator for all these coefficients, we obtain an equation $dp(x) = a'(x)b'(x)$ where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d is a nonzero element of R. If d is a unit in R, the proposition is true with $a(x) = d^{-1}a'(x)$ and $b(x) = b'(x)$. Assume d is not a unit and write d as a product of irreducibles in R, say $d = p_1 \cdots p_n$. Since p_1 is irreducible in R, the ideal (p_1) is prime, so by the theorem above, the ideal $p_1R[x]$ is prime in $R[x]$ and $(R/p_1R)[x]$ is an integral domain. Reducing the equation $dp(x) = a'(x)b'(x)$ modulo p_1, we obtain the equation $0 = \overline{a'(x)b'(x)}$ in this integral domain (the bars denote the images of these polynomials in the quotient ring), hence one of the two factors, say $\overline{a'(x)}$ must be 0. But this means all the coefficients of $a'(x)$ are divisible by p_1, so that $\frac{1}{p_1}a'(x)$ also has coefficients in R. In other words, in the equation $dp(x) = a'(x)b'(x)$ we can cancel a factor of p_1 from d (on the left) and from either $a'(x)$ and $b'(x)$ (on the right) and still have an equation in $R[x]$. But now the factor d on the left hand side has one fewer irreducible factors. Proceeding in the same fashion with each of the remaining factors of d, we can cancel all of the factors of f into the two polynomials on the right hand side, leaving an equation $p(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and with $a(x), b(x)$ being F-multiples of $A(x), B(x)$, respectively. This completes the proof. □

Theorem: (Eisenstein's Criterion)

Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + a_1x + a_0$ be a polynomial in $R[x]$ with $n \geq 1$. Suppose $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then, $f(x)$ is irreducible in $R[x]$.

Proof:

Suppose $f(x)$ were reducible, say $f(x) = a(x)b(x)$ in $R[x]$, where $a(x)$ and $b(x)$ are nonconstant polynomials. Reducing this equation modulo P and using the assumptions on the coefficients of $f(x)$, we obtain the equation

$$x^n = \overline{a(x)b(x)} \in (R/P)[x],$$

where the bar denotes the polynomials with coefficients reduced mod P. Since P is a prime ideal, R/P is an integral domain, and it follows that both $\overline{a(x)}$ and $\overline{b(x)}$ have 0 constant term, i.e., the constant terms of both $a(x)$ and $b(x)$ are elements of P. But then the constant term a_0 of $f(x)$ as the product of these two would be an element of P^2, a contradiction. Hence, $f(x)$ is irreducible. □

2.3 Modules

Theorem:

Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then, the following are equivalent:

(1) The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by

$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$

is an isomorphism (of R-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

(2) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, 2, \ldots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

Proof:

To prove that (1) implies (2), suppose that for some j that (2) fails to hold and let $a_j \in (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_l) \cap N_j$, with $a_j \neq 0$. Then,

$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$$

for some $a_i \in N_i$, and $(a_1, \ldots, a_{j-1}, -a_j, a_{j+1}, \ldots, a_k)$ would be a nonzero element of $\mathrm{Ker}(\pi)$, a contradiction.

Assume now that (2) holds. If for some module elements, $a_i, b_i \in N_i$ we have

$$a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k$$

then for each j we have

$$a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k).$$

The left hand side is in N_j and the right hand side belongs to $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Thus,

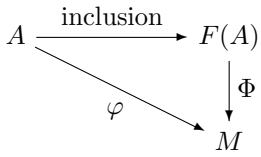
$$a_j - b_j \in N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0.$$

This shows $a_j = b_j$ for all j, and so (2) implies (3).

Finally, to see that (3) implies (1), observe first that the map π is clearly a surjective R-module homomorphism. Then (3) simply implies π is injective, hence is an isomorphism, completing the proof. □

Theorem: (Universal Property of Modules)

For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following *universal property*: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$, that is, the following diagram commutes.



When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, then $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

Proof:

Let $F(A) = \{0\}$ if $A = \emptyset$. If A is nonempty let $F(A)$ be the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$. Make $F(A)$ into an R-module by pointwise addition of functions and pointwise multiplication of a ring element times a function, i.e., for all $a \in A$, $r \in R$, and $f, g \in F(A)$:

$$(f + g)(a) = f(a) + g(a), \quad \text{and}$$

$$(rf)(a) = r(f(a)), \quad \text{for all } a \in A,\ r \in R \text{ and } f, g \in F(A).$$

It is an easy matter to check that all the R-module axioms hold. Identify A as a subset of $F(A)$ by $a \mapsto f_a$, where f_a is the function which is 1 at a and zero elsewhere. We can, in this way, think of $F(A)$ as all finite R-linear combinations of elements of A by identifying each function f with the sum $r_1a_1 + r_2a_2 + \cdots + r_na_n$, where f takes on the value r_i at a_i and is zero at all other elements of A. Moreover, each element of $F(A)$ has a unique expression as such a formal sum. To establish the universal property of $F(A)$ suppose $\varphi : A \to M$ is a map of the set A into the R-module M. Define $\Phi : F(A) \to M$ by

$$\Phi : \sum_{i=1}^{n} r_i a_i \mapsto \sum_{i=1}^{n} r_i \varphi(a_i).$$

By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the a_i we see easily that Φ is a well defined R-module homomorphism (the details are left as an exercise). By definition, the restriction of Φ to A equals φ. Finally, since $F(A)$ is generated by A, once we know the values of an R-module homomorphism on A its values on every element of $F(A)$ are uniquely determined, so Φ is the unique extension of φ to all of $F(A)$. When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, the previous theorem shows that $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Since $R \cong Ra_i$ for all i (under the map $r \mapsto ra_i$) the previous theorem shows that the direct sum is isomorphic to R^n. □

Theorem: (Every Vector Space has a Basis)

Let V be a vector space of arbitrary dimension over a field F. Prove that V has a basis (by convention the null set is the basis for the zero space).

Proof:

Let V be a vector space. If V is the zero space, then by convention it has the null set as a basis. Now assume that V is not the zero space, i.e., there exists a nonzero vector $v \in V$.

Let $\mathcal{S}$ be the set of all subsets of V containing linearly independent vectors. Let this set be partially ordered under inclusion. Consider a chain $\{T_i\}A_{i\in I}$, such that each $T_i \in \mathcal{S}$. We must write the chain in this way because it may not be countable. Define

$$T := \bigcup_{i=1}^{\infty} T_i.$$

To show that T is an upper bound for the above chain, it is necessary to show that

1: $T_i \subseteq T$, for all $i \in I$, and

2: $T \in \mathcal{S}$.

So,

(1) Let $i \in I$ be fixed. It is clear that $T_i \subseteq T$ by the definition of T.

(2) To show that $T \in \mathcal{S}$, we have to verify that T is a set of linearly independent vectors. Assume toward a contradiction that the subset $\{v_1, v_2, \ldots\} \subseteq T$ is not a linearly independent set. Since the sets T_i form a chain under inclusion, there exists a set T_m such that $\{v_1, v_2, \ldots\} \subseteq T_m$. This contradicts the assumption that $T_m \in \mathcal{S}$. Therefore, T must be a set of linearly independent vectors, and so $T \in \mathcal{S}$.

Hence we can apply **Zorn's Lemma** to conclude that $\mathcal{S}$ has a maximal element M. Since $M \in \mathcal{S}$, we automatically have that M is a linearly independent set of vectors. To show that M is a basis for V, it remains to show that M spans S.

Assume toward a contradiction that there is a vector $w \in V$ such that w is not in the span of M. Then, $M \cup \{w\}$ is a linearly independent set, which contradicts the maximality of M. Hence, M must span V. Therefore, M is a basis for V. Since V was arbitrary, we have shown that every vector space has a basis. □

Theorem: (Replacement Theorem)

Assume $\mathcal{A} := \{a_1, a_2, \ldots, a_n\}$ is a basis for V containing n elements and $\{b_1, b_2, \ldots, b_m\}$ is a set of linearly independent vectors in V. Then there is an ordering $a_1, a_2, \ldots, a_n$ such that for each $k \in \{1, 2, \ldots, m\}$, the set $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis of V. In other words, the elements $b_1, b_2, \ldots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis. In particular, $m \geq n$.

Proof:

We proceed by induction on k. If $k = 0$ there is nothing to prove, since $\mathcal{A}$ is given as basis for V. Suppose now that $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis for V. Then in particular this is a spanning set, so b_{k+1} is a linear combination:

$$b_{k+1} = \beta_1 b_1 + \cdots + \beta_k b_k + \alpha_{k+1} a_{k+1} + \cdots + \alpha_n a_n.$$

Not all of the α_i can be 0, since this would imply b_{k+1} is a linear combination of $b_1, b_2, \ldots, b_k$, contrary to the linear independence of these elements. By reordering if necessary, we may assume $\alpha_{k+1} \neq 0$. Then solving this last equation for a_{k+1} as a linear combination of b_{k+1} and $b_1, b_2, \ldots, b_k, a_{k+2}, \ldots, a_n$ shows

$$\text{Span}\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\} = \text{Span}\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$$

and so this is a spanning set for V. It remains to show $b_1, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n$ are linearly independent. If

$$\beta_1 b_1 + \cdots + \beta_k b_k + \beta_{k+1} b_{k+1} + \alpha_{k+2} a_{k+2} + \cdots + \alpha_n a_n = 0$$

then substituting for b_{k+1} from the expression for b_{k+1} above, we obtain a linear combination of $\{b_1, b_2, \ldots, b_k, a_{k+1}, a_{k+2}, \ldots, a_n\}$ equal to 0, where the coefficient of a_{k+1} is β_{k+1}. Since this last set is a basis by induction, all the coefficients in this linear combination, in particular β_{k+1}, must be 0. But then from above we have

$$\beta_1 b_1 + \cdots + \beta_k b_k + \alpha_{k+2} a_{k+2} + \cdots + \alpha_n a_n = 0.$$

Again by the induction hypothesis all the other coefficients must be 0 as well. Thus $\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis for V, and the induction is complete. □

Theorem: (Rank-Nullity Theorem)

Let V be a vector space over F and let W be a subspace of V. Then V/W is a vector space with $\dim(V) = \dim(W) + \dim(V/W)$ (where if one side is infinite then both are).

Proof:

Suppose W has dimension m and V has dimension n over F and let $w_1, w_2, \ldots, w_m$ be a basis for W. By the **Building-Up Lemma**, these linearly independent elements of V can be extended to a basis $w_1, w_2, \ldots, w_m, v_{m+1}, \ldots, v_n$ of V. The natural surjective projection map of V into V/W maps each w_i to 0. No linear combination of the v_i is mapped to 0, since this would imply this linear combination is an element of W, contrary to the choice of the v_i. Hence, the image V/W of this projection map is isomorphic to the subspace of V spanned by the v_i, and so $\dim(V/W) = n - m$, which is the theorem when the dimensions are finite. If either side is infinite, it is easy to produce an infinite number of linearly independent vectors showing the other side is also infinite. □

Theorem: (Basis of a Dual Space)

Let $\mathcal{B} := \{v_1, v_2, \ldots, v_n\}$ be a basis of the finite dimensional vector space V. Define $v_i^* \in V^*$ by its action on the basis $\mathcal{B}$:

$$v_i^*(v_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \qquad 1 \leq j \leq n.$$

Then, $\{v_1^*, v_2^*, \ldots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional, then V^* has the same dimension as V.

Proof:

Observe that since V is finite dimensional, $\dim(V^*) = \dim(\text{Hom}_F(V, F)) = \dim(V)\dim(F) = n \cdot 1 = n$, so since there are n of the $v_i^* s$ it suffices to prove that they are linearly independent. If

$$\alpha_1 v_1^* + \cdots + \alpha_n v_n^* = 0$$

in $\text{Hom}_F(V, F)$, then applying this element to v_i we obtain $\alpha_i = 0$. Since i is arbitrary, these elements are linearly independent. □

Theorem: (Isomorphism Between V and V^{**})

There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional, then this linear transformation is an isomorphism.

Proof:

Let $v \in V$, Define the map *evaluation at* v by

$$E_v : V^* \to F \qquad \text{by} \qquad E_v(f) = f(v).$$

Then $E_v(f + \alpha g) = (f + \alpha g)(v) = f(v) + \alpha g(v) = E_v(f) + \alpha E_v(g)$, so that E_v is a linear transformation from V^* to F. Hence, E_v is an element of $\mathrm{Hom}_F(V^*, F) = V^{**}$. This defines a natural map

$$\varphi : V \to V^{**} \qquad \text{by} \qquad \varphi(v) = E_v.$$

The map φ is a *linear* map, as follows: for $v, w \in V$ and $\alpha \in F$,

$$E_{v+\alpha w}(f) = f(v + \alpha w) = f(v) + \alpha f(w) = E_v(f) + \alpha E_w(f)$$

for every $f \in V^*$, and so

$$\varphi(v + \alpha w) = E_{v+\alpha w} = E_v + \alpha E_w = \varphi(v) + \alpha\varphi(w).$$

To see that φ is injective, let v be any nonzero vector in V. By the **Building Up Lemma**, there is a basis $\mathcal{B}$ containing v. Let f be the linear transformation from V to F define by sending v to 1 and every element of $\mathcal{B} \setminus \{v\}$ to zero. Then $f \in V^*$ and $E_v(f) = f(v) = 1$. Thus $\varphi(v) = E_v$ is not zero in V^{**}. This proves $\mathrm{Ker}(\varphi) = 0$, i.e., φ is injective.

If V has finite dimension n, then by the above proof, V^* and hence also V^{**} have dimension n. In this case φ is an injective linear transformation from V to a finite dimensional vector space off the same dimension, hence is an isomorphism. □

Theorem:

Let S and T be linear transformations of V. Then the following are equivalent:

(1) S and T are similar linear transformations.

(2) The $F[x]$-modules obtains from V via S and via T are isomorphic $F[x]$-modules.

(3) S and T have the same rational canonical form.

Proof:

Assume that (1) holds. Let U be the nonsingular linear transformation U such that $S = UTU^{-1}$. The vector space isomorphism $U : V \to V$ is also an $F[x]$-module homomorphism, where x acts on the first V via T and on the second via S, since for example $U(xv) = U(T(x)) = UT(v) = SU(v) = x(Uv)$. Hence this is an $F[x]$-module isomorphism of the two modules in (2). So, (2) holds.

Let (2) hold. Denote by V_1 the vector space V made into an $F[x]$-module via S and denote by V_2 the vector space V made into an $F[x]$-module via T. Since $V_1 \cong V_2$, as $F[x]$-modules they have the same list of invariant factors. Thus, S and T have a common Rational Canonical Form. So, (3) holds.

Lastly, assume (3) holds. Since S and T have the same matrix representation with respect to some choice of (possibly different) bases of V by assumption, they are, up to a change of basis, the same linear transformation of V, hence are similar. So, (1) holds. □

2.4 Fields

Theorem:

Every field F contains a unique smallest subfield F_0 and F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof:

Let $\mathscr{F}$ be the set of all subfields of F. Define

$$F_0 := \bigcap_{K \in \mathscr{F}} K.$$

First, note that F_0 is a subfield of F because the arbitrary intersection of rings is a ring and every nonzero element in F_0 is in every subfield of F and so has an inverse in every subfield of F (the same inverse, since inverses are unique) and so an inverse in F_0. Moreover, F_0 is the unique smallest subfield because it is contained in every other subfield.

To see that either $F_0 \cong \mathbb{Z}/p\mathbb{Z}$ or $F_0 \cong \mathbb{Q}$, consider the homomorphism

$$\varphi : \mathbb{Z} \to F_0$$

defined by $\varphi(n) = n \cdot 1_F$. If F has characteristic 0, then φ is injective and we can extend φ to an injection from $\mathbb{Q}$ to F_0. Observing that $\operatorname{Im}\varphi$ is a subfield of F, we must have that $\operatorname{Im}(\varphi) = F_0$, i.e., φ is an isomorphism and so in this case $F_0 \cong \mathbb{Q}$. If F has characteristic p, then the induced map $\overline{\varphi} : \mathbb{Z}/p\mathbb{Z} \to F_0$ is an injective homomorphism with $\operatorname{Im}(\overline{\varphi}) = F_0$, and so again $\overline{\varphi}$ is an isomorphism. So, in this case $F_0 \cong \mathbb{Z}/p\mathbb{Z}$. □

Theorem:

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then, there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.

Proof:

Consider the quotient

$$K := F[x]/(p(x))$$

of the polynomial ring $F[x]$ by the ideal generated by $p(x)$. Since by assumption $p(x)$ is an irreducible polynomial in the Principal Ideal Domain $F[x]$, the ideal $(p(x))$ is a maximal ideal. Hence K is actually a field. The canonical projection π of $F[x]$ to the quotient $F[x]/(p(x))$ restricted to $F \subset F[x]$ gives a homomorphism $\varphi = \pi\big|_F : F \to K$ which is not identically 0 since it maps the identity 1 of F to the identity 1 of K. Hence by the proposition above, $\varphi(F) \cong F$ is an isomorphic copy of F contained in K. We identity F with its isomorphic image in K, and view F as a *subfield* of K. If $\overline{x} = \pi(x)$ denotes the image of x in the quotient K, then

$$\begin{aligned} p(\overline{x}) &= \overline{p(x)} \\ &= p(x) \pmod{p(x)} \\ &= 0 \end{aligned}$$

so that K does indeed contain a root of the polynomial $p(x)$. Then K is an extension of F in which the polynomial $p(x)$ has a root. □

Theorem:

Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta := x \pmod{(p(x))} \in K$. Then the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $\big[K : F\big] = n$. Hence

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}$$

consists of all polynomials of degree $< n$ in θ.

Proof:

Let $a(x) \in F[x]$ be any polynomial with coefficients in F. Since $F[x]$ is a Euclidean Domain, we may divide $a(x)$ by $p(x)$:

$$a(x) = q(x)p(x) + r(x) \qquad q(x), r(x) \in F[x] \text{ with } \deg(r(x)) < n.$$

Since $q(x)p(x)$ lies in the ideal $(p(x))$, it follows that $a(x) \equiv r(x) \pmod{(p(x))}$, which shows they every residue class in $F[x]/(p(x))$ is represented by a polynomial of degree less than n. Hence the images $1, \theta, \theta^2, \ldots, \theta^{n-1}$ of $1, x, x^2, \ldots, x^{n-1}$ in the quotient *span* the quotient as a vector space over F. It remains to see that these elements are linearly independent, so form a basis for the quotient over F.

If the elements $1, \theta, \theta^2, \ldots, \theta^{n-1}$ were not linearly independent in K, then there would be a linear combination

$$b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} = 0$$

in K, with $b_0, b_1, \ldots, b_{n-1} \in F$ not all 0. This is equivalent to

$$b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} \equiv 0 \pmod{(p(x))}$$

i.e.,

$$p(x) \mid b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$$

in $F[x]$. But this is impossible, since $p(x)$ is of degree n and the degree of the nonzero polynomial on the right is $< n$. This proves that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis for K over F, so that $\big[K : F\big] = n$ by definition. The last statement follows immediately. □

Theorem:

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$, i.e., $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

$$F(\alpha) \cong F[x]/(p(x)).$$

Proof:

There is a natural homomorphism $\varphi : F[x] \to F(\alpha) \subseteq K$ define by $\varphi(a(x)) = a(\alpha)$ obtained by mapping F to F by the identity map and sending x to α, and the ending so that the map is a ring homomorphism (i.e., the polynomial $a(x)$ in x maps to the polynomial $a(\alpha)$ in α). Since $p(\alpha) = 0$ by assumption, the element $p(x)$ is in the kernel of φ, so we obtain an induced homomorphism (also denoted φ):

$$\varphi : F[x]/(p(x)) \to F(\alpha).$$

But since $p(x)$ is irreducible, the quotient on the left is a field, and φ is not the 0 map (it is the identity on F, for example), hence φ is an isomorphism of the field on the left with its image. Since this image is then a subfield of $F(\alpha)$ containing F and containing α, by the definition of $F(\alpha)$ the map must be surjective, proving the theorem. □

Theorem:

Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism $\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$ defined by $\sigma(\alpha) = \beta$, which maps α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

Proof:

The isomorphism φ induces a natural isomorphism from $F[x]$ to $F'[x]$ which maps the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$. Taking the quotients by these ideals, we obtain an isomorphism of fields

$$F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x)).$$

By the above theorem, the field on the left is isomorphic to $F(\alpha)$, which the field on the right is isomorphic to $F'(\beta)$. Composing these isomorphisms, we obtain the isomorphism σ. It is clear that the restriction of this isomorphism to F is φ, completing the proof. □

Theorem:

Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Proof:

Let $g(x) \in F[x]$ be a polynomial of minimal degree having α as a root. Multiplying $g(x)$ by a constant, we may assume $g(x)$ is monic. Suppose $g(x)$ were reducible in $F[x]$, say $g(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$ both of degree smaller than the degree of $g(x)$. Then $g(\alpha) = a(\alpha)b(\alpha)$ in K, and since K is a field, either $a(\alpha) = 0$ or $b(\alpha) = 0$, contradicting the minimality of the degree of $g(x)$. It follows that $g(x)$ is a monic irreducible polynomial having α as a root. Suppose now that $f(x) \in F[x]$ is any polynomial having α as a root. By the Euclidean Algorithm in $F[x]$, there are polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r(x)) < \deg(g(x))$. Then, $f(\alpha) = q(\alpha)g(\alpha) + r(\alpha)$ in K and since α is a root of both $f(x)$ and $g(x)$, we obtain $r(\alpha) = 0$, which contradicts the minimality of $g(x)$ unless $r(x) = 0$. Hence, $g(x)$ divides any polynomial $f(x)$ in $F[x]$ having α as a root and, in particular, would divide any other monic irreducible polynomial in $F[x]$ having α as a root. This proves that $m_{\alpha,F}(x) = g(x)$ is unique and completes the proof of the proposition. □

Theorem:

The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is at most n.

Proof:

If α is algebraic over F, then the degree of the extension $F(\alpha)/F$ is the degree of the minimal polynomial for α over F. Hence the extension is finite, of degree $\leq n$ if α satisfies a polynomial of degree n. Conversely, suppose α is an element of an extension of degree n over F (for example, if $\big[F(\alpha) : F\big] = n$). Then the $n+1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ of $F(\alpha)$ are linearly dependent over F, say $b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$, with $b_0, b_1, b_2, \ldots, b_n \in F$ not all 0. Hence α is the root of a nonzero polynomial with coefficients in F (of degree $\leq n$), which proves α is algebraic over F and also proves the second statement of the proposition. □

Theorem:

Let $F \subseteq K \subseteq L$ be fields. Then

$$\big[L : F\big] = \big[L : K\big]\big[K : F\big],$$

i.e., extension degrees are multiplicative, where if one side of the equation is infinite, the other side is also infinite. Pictorially,

$$\overbrace{\underbrace{F \quad \subseteq}_{[K:F]} \quad K \quad \underbrace{\subseteq \quad L}_{[L:K]}}^{[L:F]}$$

Proof:

Suppose first that $\big[L : K\big] = m$ and $\big[K : F\big] = n$ are finite. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be a basis for L over K and let $\beta_1, \beta_2, \ldots, \beta_n$ be a basis for K over F. Then every element of L can be written as a linear combination

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m$$

where $a_1, \ldots, a_m$ are elements of K, hence are F-linear combinations of $\beta_1, \ldots, \beta_n$:

$$a_i = b_{i,1}\beta_1 + \cdots + \beta_{i,n}\beta_n, \qquad i = 1, 2, \ldots, m$$

where the $b_{i,j}$ are elements of F. Substituting these expressions in for the coefficients a_i above, we see that every element of L can be written as a linear combination

$$\sum_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} b_{i,j}\alpha_i\beta_j$$

of the mn elements $\alpha_i\beta_j$ with coefficients in F. Hence these elements span L as a vector space over F. Suppose now that we had a linear relation in L

$$\sum_{\substack{i=1,2,\ldots,m \\ j=1,2,\ldots,n}} b_{i,j}\alpha_i\beta_j = 0$$

with coefficients $b_{i,j}$ in F. Then defining the elements $a_i \in K$ by the equation above, this linear relation could be written

$$a_1\alpha_1 + \cdots + a_m\alpha_m = 0.$$

Since the α_i are a basis for L over K, it follows that all the coefficients a_i must be 0, i.e. that

$$b_{i,1}\beta_1 + \cdots + \beta_{i,n}\beta_n = 0$$

in K. Since now the β_j form a basis for K over F, this implies that $b_{i,j} = 0$ for all i and j. Hence the elements $\alpha_i\beta_j$ are linearly independent over F, so form a basis for L over F and $\big[L : F\big] = mn = \big[L : K\big]\big[K : F\big]$, as claimed. □

Theorem:

$F(\alpha, \beta) = (F(\alpha))(\beta)$, i.e., the field generated by F of α and β is the field generated by β over the field $F(\alpha)$ generated by α.

Proof:

This follows by the minimality of the fields in question. The field $F(\alpha, \beta)$ contains F and α, hence contains the field $F(\alpha)$, and since it also contains β, we have the inclusion $(F(\alpha))(\beta) \subseteq F(\alpha, \beta)$ by the minimality of the field $(F(\alpha))(\beta)$. Since the field $(F(\alpha))(\beta)$ contains F, α, and β, by the minimality of $F(\alpha, \beta)$ we have the reverse inclusion $F(\alpha, \beta) \subseteq (F(\alpha))(\beta)$, which proves the theorem. □

Theorem:

If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Proof:

Let α be any element of L. Then α is algebraic over K, so α satisfies some polynomial equation

$$a_n\alpha^n + a_{n-1}\alpha^{n-2} + \cdots + a_1\alpha + a_0 = 0$$

where the coefficients $a_0, a_1, \ldots, a_n$ are in K. Consider the field $F(\alpha, a_0, a_1, \ldots, a_n)$ generated over F by α and the coefficients of this polynomial. Since K/F is algebraic, the elements $a_0, a_1, \ldots, a_n$ are algebraic over F, so the extension $F(a_0, a_1, \ldots, a_n)/F$ is finite. By the equation above, we see that α generates an extension of this field of degree at most n, since its minimal polynomial over this field is a divisor of the polynomial above. Therefore,

$$\big[F(\alpha, a_0, \ldots, a_n) : F\big] = \big[F(\alpha, a_0, \ldots, a_n) : F(a_0, \ldots, a_n)\big]\big[F(a_0, \ldots, a_n) : F\big]$$

is also finite and $F(\alpha, a_0, a_1, \ldots, a_n)/F$ is an algebraic extension. In particular the element α is algebraic over F, which proves that L is algebraic over F. □

Theorem: (Existence of Splitting Fields)

For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.

Proof:

We first show that there is an extension E of F over which $f(x)$ splits completely into linear factors by induction on the degree n of $f(x)$. If $n = 1$, then take $E = F$. Suppose now that $n > 1$. If the irreducible factors of $f(x)$ over F are all of degree 1, then F is the splitting field for $f(x)$ and we may take $E = F$. Otherwise, at least one of the irreducible factors, say $p(x)$ of $f(x)$ in $F[x]$ is of degree at least 2. Hence, there is an extension E_1 of F containing a root α of $p(x)$. Over E_1 the polynomial $f(x)$ has the linear factor $x - \alpha$. The degree of the remaining factor $f_1(x)$ of $f(x)$ is $n - 1$, so by induction there is an extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E$, E is an extension of F containing all the roots of $f(x)$. Now let K be the intersection of all the subfields of E containing F which also contain all the roots of $f(x)$. Then, K is a field which is a splitting field for $f(x)$. □

Chapter 3

Popular Examples & Counterexamples

3.1 Rings

Example: (A Principal Ideal Domain which is not a Euclidean Domain)

Let R be an integral domain. Define $\widetilde{R} := R^\times \cup \{0\}$. Recall than an element $u \in R \setminus \widetilde{R}$ is called a *universal side divisor* if for every $x \in R$ there is some $z \in \widetilde{R}$ such that u divides $x - z$ in R.

Now let R be a Euclidean Domain with some norm N and let u be an element of $R \setminus \widetilde{R}$ with minimal norm. For any $x \in R$, we can use the division algorithm to pick $q, r \in R$ such that $x = qu + r$ where $r = 0$ or $N(r) < N(u)$. By the minimality of u, we have $r \in \widetilde{R}$ and so u is a universal side divisor in R. Therefore, every Euclidean Domain has universal side divisors.

Consider the ring $R := \mathbb{Z}[(1 + \sqrt{-19})/2]$. We will show that R is not a Euclidean Domain by showing that R has no universal side divisors. We know from the study of quadratic integer rings that the only units of R are ± 1 and so $\widetilde{R} = \{0, \pm 1\}$. Let N be the field norm on R, so that

$$N(a + b(1 + \sqrt{-19})/2) = a^2 + ab + 5b^2$$

and observe that if $a, b \in \mathbb{Z}$ with $b \neq 0$, we have that $N(a + b(1 + \sqrt{-19})/2) \geq 5$. In fact, the only elements of R with norm less than 5 are $\pm 1, \pm 2$ with $N(\pm 1) = 1$ and $N(\pm 2) = 4$.

Let $x = 2$ in the definition of universal side divisors. Then a universal side divisor u must divide 1, 2, or 3. Since u is not a unit, either $u \mid 2$ or $u \mid 3$. If the element 2 factors as $2 = \alpha\beta$, then $4 = N(\alpha)N(\beta)$ and so by the remark above either α or β is a unit. So, the divisors of 2 are $\{\pm 1, \pm 2\}$. Similarly, the divisors of 3 are $\{\pm 1, \pm 3\}$. Hence, $u \in \{\pm 2, \pm 3\}$. Now let $x := (1 + \sqrt{-19})/2$. It remains to check that the elements $x - 1$, x, $x + 1$ are not divisible by ± 2 or ± 3. Hence, there can be no universal side divisors of R and so R is not a Euclidean Domain. It remains to show that R is a Principal Ideal Domain.

Recall that a map $N : R \to \mathbb{Z}$ is a *Dedekind-Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$, either a is an element of (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than $N(b)$ (i.e., either $b \mid a$ in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).

Let R be an integral domain with a Dedekind-Hasse norm N. Let I be an ideal of R. Let b be a nonzero element of I with $N(b)$ minimal. Let a be any nonzero element in I so that $(a, b) \subseteq I$. The minimality of $N(b)$ implies that $a \in (b)$ and so I is principal. Hence, any integral domain with a Dedekind-Hasse norm is a Principal Ideal Domain. Now, see **Dummit & Foote, pg. 282** for an argument that the field norm of this quadratic integer ring is a Dedekind-Hasse norm.

Thus, we can conclude that $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a Principal Ideal Domain, but not a Euclidean Domain.

Example: (A Unique Factorization Domain which is not a Principal Ideal Domain)

Recall that $R[x]$ is a Unique Factorization Domain if and only if R is a Unique Factorization Domain. Therefore, $\mathbb{Z}[x]$ is a Unique Factorization Domain. However, consider the ideal $(2, x) \in \mathbb{Z}[x]$. This ideal is clearly not principal because if it were, there would be a polynomial $d(x) \in R[x]$ that divides both 2 and x, which would give $d(x) = \pm 1$, i.e., $(2, x) = \mathbb{Z}[x]$. However, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$, and so $(2, x) \neq \mathbb{Z}[x]$. So, $\mathbb{Z}[x]$ is a Unique Factorization Domain, but not a Principal Ideal Domain. $\square$

Chapter 4

Past Exams

4.1 January 1997

1 (a) Prove that there are exactly four homomorphisms from Z_2 into $\mathrm{Aut}(Z_8)$.

(b) Show that these yield four pairwise nonisomorphic semidirect products.

Proof: See **First Year Pool, Exercise 23**.

2 State and probe the Orbit-Stabilizer Theorem.

Proof: See **First Year Pool, Exercise 38**.

3 Suppose that $|G| = 105$. If G has a normal Sylow 3-subgroup, probe that it must lie in the center of G and that G is solvable.

Proof: See **First Year Pool, Exercise 46**.

4 Let F be a field and $A = F[[x]]$ denote the ring of formal power series in one variable. Prove the following:

(a) The units of A are precisely the power series whose constant term is nonzero.

(b) Let I_k denote the set of all power series $\sum a_n x^n$ for which $a_0, \ldots, a_{k-1}$ are all zero. Prove that each I_k is an ideal of A, and that these are the only nonzero ideals of A.

Proof: See **First Year Pool, Exercise 53**.

5 Prove the Division Algorithm for the ring $\mathbb{Z}[i]$ of Gaussian integers.

Proof: See **First Year Pool, Exercise 54**.

6 Let n be a natural number; prove that the polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1}$$

is irreducible over the ring $\mathbb{Z}$ precisely when n is prime.

Proof: See **First Year Pool, Exercise 67**.

7 Suppose that $T : V \to W$ is a linear transformation between vector spaces over the same field F. Prove that T is one to one prcisely when it maps linearly independent sets to linearly independent sets.

Proof: See **First Year Pool, Exercise 78**.

8 Let R be a ring with identity. Suppose that $\varphi : M \to F$ is a surjective R-homomorphism and that F is a free R-module. Prove that $M = \mathrm{Ker}(\varphi) \oplus N$, where $N \cong F$.

Proof: See **First Year Pool, Exercise 84**.

9 Prove that in $GL_2(\mathbb{Q})$ all the elements of order four are conjugate. (Hint: Consider the rational canonical form of such an element.)

Proof: See **First Year Pool, Exercise 89**.

10 Let F be a field and suppose that K is a field extension of F, Prove that the set of elements of K which are algbraic over F form a subfield of K containing F.

Proof: See **First Year Pool, Exercise 110**.

4.2 May 1997

1 Prove that a group of order 30 must have a normal subgroup of order 15.

Proof: See **First Year Pool, Exercise 17**.

2 Prove that D_{2n} is nilpotent if and only if n is a power of 2. (Hint: Use the upper central series; show that if $n \geq 3$ then $Z(D_{2n}) \neq \{1\}$ if and only if n is even.)

Proof: See **First Year Pool, Exercise 26**.

3 Let $\mathbb{C}$ be the field of complex numbers. Prove that each irreducible $\mathbb{C}[x]$-module is isomorphic to $\mathbb{C}$.

Proof: See **First Year Pool, Exercise 103**.

4 Suppose that A is a commutative ring with identity, and I is an ideal of A.

(a) For each positive integer n, prove that

$$A^n/IA^n \cong A/I \times \cdots \times A/I.$$

(b) Use (a) to prove that if $A^m \cong A^n$, where m and n are positive integers, then $m = n$. (You may use the corresponding fact for fields.)

Proof: See **First Year Pool, Exercise 73**.

5 Prove that $X^2 + Y^2 - 1$ is irreducible in $\mathbb{Q}[X, Y]$. (Hint: Translate by a suitable quantity and then apply the general form of Eisenstein's Criterion.)

Proof: See **First Year Pool, Exercise 68**.

6 Let R be a UFD.

(a) Define what it means for $f(x) \in R[x]$ to be a primitive polynomial.

(b) Let $f, g \in R[x]$. Prove that fg is primitive if and only if f and g are both primitive.

Proof:

For (a) and the ($\Longleftarrow$) direction of (b), see **First Year Pool, Exercise 62**.

($\Longrightarrow$) :

Let $f, g \in R[x]$. Let fg be primitive. Assume toward a contradiction that f or g (without loss of generality, say f) is not primitive. Let p be a prime that divides every coefficient of f. Since every coefficient of fg is a sum of products of a coefficient of f and a coefficient of g, we have that p divides every coefficient of fg, which contradicts the assumption that fg is primitive. Therefore, f and g are both primitive. $\square$

7 Let V be a vector space over a field F. Prove that V has a basis. (Do not assume that V is finitely generated.)

Proof: See **Important Theorems - Modules**.

8 Find a representative for every conjugacy class of elements of order 5 in $GL_8(\mathbb{Q})$.

Proof:

Let A be an element of order 5 in $GL_8(\mathbb{Q})$. Then, $A^5 - I = 0$ and $A - 1 \neq= 0$. Since $A^5 - 1 = (A-1)(A^4 + A^3 + A^2 + A + 1)$, the possibilities for the minimal polynomial are

$$m_1(x) = x^5 - 1,$$
$$m_2(x) = x^4 + x^3 + x^2 + x + 1.$$

Hence, the possible invariant factor lists are

$$x^5 - 1, \;\; x - 1, \;\; x - 1, \;\; x - 1,$$

$$x^4 + x^3 + x^2 + x + 1, \;\; x^4 + x^3 + x^2 + x + 1$$

The corresponding rational canonical forms are:

$$\begin{pmatrix} (1) & & & & \\ & (1) & & & \\ & & (1) & & \\ & & & \begin{pmatrix} 0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0 \end{pmatrix} \end{pmatrix}, \quad \begin{pmatrix} \begin{pmatrix} 0&0&0&-1\\1&0&0&-1\\0&1&0&-1\\0&0&1&-1\\0&0&0&-1 \end{pmatrix} & \\ & \begin{pmatrix} 0&0&0&-1\\1&0&0&-1\\0&1&0&-1\\0&0&1&-1\\0&0&0&-1 \end{pmatrix} \end{pmatrix}.$$

Hence, these are the two representatives for the two conjugacy classes of elements of order 5 in $GL_8(\mathbb{Q})$. □

9 Determine all homomorphisms $\varphi : Z_3 \to \mathrm{Aut}(Z_9)$ and construct the associated semidirect products. Prove that the semidirect products associated to the non-trivial homomorphisms are all isomorphic.

Proof:

Let $Z_3 = \langle x \rangle$ and let $Z_9 = \langle y \rangle$. Note that $\mathrm{Aut}(Z_9)$ has order 6. The six elements of $\mathrm{Aut}(Z_9)$ are $\Phi_i : y \mapsto y^i$ for $i \in \{1, 2, 4, 5, 7, 8\}$. Note that Φ_1 is the identity, and that in fact $\mathrm{Aut}(Z_9)$ is cyclic with Φ_2 as a generator. Hence, the elements of order 3 in $\mathrm{Aut}(Z_9)$ are $(\Phi_2)^2 = \Phi_4$ and $(\Phi_2)^4 = \Phi_7$. If φ is a non-trivial homomorphism from Z_3 to $\mathrm{Aut}(Z_9)$, then φ is completely determined by $\varphi(x)$, which must be an element of order three in $\mathrm{Aut}(Z_9)$. Hence, the possible non-trivial homomorphisms are

$$\varphi_1 : x \mapsto [y \mapsto y^4]$$

$$\varphi_2 : x \mapsto [y \mapsto y^7]$$

Note that $\varphi_1(x) = \varphi_2(x^2)$ and that $\varphi_1(x^2) = \varphi_2(x)$. Hence, φ_1 and φ_2 differ by an automorphism of Z_3 which swaps x and x^2 and therefore the semidirect products coming from each homomorphism are isomorphic. (Another way of saying this is that the difference between x and x^2 is just an arbitrary choice of generator, and the semidirect product arising from each choice is the same.) □

10 Prove that every field F contains a unique smallest subfield F_0, and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof:

See **Important Theorems - Fields**.

4.3 August 1997

1 Let R be a commutative ring and let I be an ideal in R. Prove that $I[x]$ is an ideal in $R[x]$ and that $R[x]/I[x] \cong (R/I)[x]$.

Proof:

It is clear that $I[x]$ is contained in $R[x]$. Let $f(x), g(x) \in I[x]$. Then, all coefficients of $f(x)+g(x)$ lie in $I[x]$, and so $f(x) + g(x) \in I[x]$. Let $r(x) \in R[x]$ and consider $r(x)f(x)$. Each coefficient of

$r(x)f(x)$ is a sum of products ab where $a \in R$ and $b \in I$. Since I is an ideal of R, $ab \in I$ and so the sum of these products is in I. Thus, $r(x)f(x) \in I[x]$ and so $I[x]$ is an ideal of $R[x]$.

To see the isomorphism, consider the reduction homomorphism

$$\varphi : R[x] \to (R/I)[x]$$

that takes a polynomial and reduces the coefficients modulo I. Observe that $f(x) \in \text{Ker}(\varphi)$ if and only if every coefficient of $f(x)$ is in I, i.e., $\text{Ker}(\varphi) = I[x]$. Additionally, φ is clearly surjective since the reduction map $R \to R/I$ is surjective. Therefore, by the **First Isomorphism Theorem of Rings**, we have that $R[x]/I[x] \cong (R/I)[x]$. $\square$

2 State and prove Eisenstein's criterion for the irreducibility of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Proof: See **Important Theorems - Rings**.

3 Let $k \leq n$ and let $\sigma = (1\ 2\ \cdots\ k)$ be a k-cycle in the symmetric group S_n. Describe the conjugacy class of σ and the centralizer of σ explicitly. Justify your answers.

Proof:

See **First Year Pool, Exercise 3a** for a proof that the conjugacy class of any k-cycle is exactly the subgroup of all k-cycles. Now, I claim that

$$C_{S_n}(\sigma) = \{\sigma^i \tau \mid 0 \leq i < k,\ \tau \text{ fixes } 1, 2, \ldots, k\}.$$

It is clear that every permutation in that set is in the centralizer of S_n because σ commutes with all powers of itself as well as with permutations that fix $1, 2, \ldots, k$. To see that this set contains every element that centralizes σ first observe that it has cardinality $k \cdot (n-k)!$. Now, by the **Orbit Stabilizer Theorem** applied to the action on conjugation:

$$\begin{aligned}
|S_n| &= |\,\text{Orb}(\sigma)| \cdot |\,\text{Stab}(\sigma)| \\
n! &= |\{\text{conjugacy class of } \sigma\}| \cdot |C_{S_n}(\sigma)| \\
n! &= |\{\text{all } k\text{-cycles}\}| \cdot |C_{S_n}(\sigma)| \\
n! &= \binom{n}{k} \cdot (k-1)! \cdot |C_{S_n}(\sigma)| \\
n! &= \frac{n!}{k \cdot (n-k)!} \cdot |C_{S_n}(\sigma)| \\
|C_{S_n}(\sigma)| &= k \cdot (n-k)!.
\end{aligned}$$

Hence the given set must contain all centralizing elements of σ. $\square$

4 Let R be a commutative ring with 1.

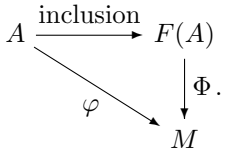
(a) Let S be a set and let $F(S)$ be the free R-module on S. State the universal mapping theorem for $F(S)$.

(b) Prove that for any R-module M there is a free R-module F and an onto R-module homomorphism $\varphi : F \to M$.

Proof:

Let S be a set and $F(S)$ be the free R-module on S. The universal mapping theorem for $F(S)$ says that if M is any R-module and $\varphi : S \to M$ is any map (of sets), then there exists a unique

R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$, i.e., the following diagram commutes:



Let M be an R-module. Consider M as a set with $\varphi : M \to M$ as the identity map. By the universal mapping theorem on $F := F(M)$, there exists a unique R-module homomorphism $\Phi : F \to M$ with $\Phi(m) = \varphi(m) = m$, which shows that Φ is onto. $\square$

5 Find a single representative for each conjugacy class of elements of order 4 in $GL_2(\mathbb{Z}/5\mathbb{Z})$.

Proof:

Let A be an element of order 4 in $GL_2(\mathbb{Z}/5\mathbb{Z})$, so that $A^4 = 1$ but $A^2 \neq 1$ and $A \neq 1$. Note that in $\mathbb{Z}/5\mathbb{Z}$, we can factor $x^4 - 1 = (x+1)(x+2)(x+3)(x+4)$. So, we have the following possibilities for the minimal polynomial of A:

$$\begin{aligned}
m_1(x) &= (x+1)(x+2),\\
m_2(x) &= (x+1)(x+3),\\
m_3(x) &= (x+2)(x+3),\\
m_4(x) &= (x+2)(x+4),\\
m_5(x) &= (x+3)(x+4),\\
m_6(x) &= (x+2),\\
m_7(x) &= (x+3).
\end{aligned}$$

The corresponding invariant factor lists are

$$\begin{aligned}
&(x+1)(x+2),\\
&(x+1)(x+3),\\
&(x+2)(x+3),\\
&(x+2)(x+4),\\
&(x+3)(x+4),\\
&(x+2),\ \ (x+2),\\
&(x+3),\ \ (x+3).
\end{aligned}$$

The corresponding rational canonical forms are

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

$$\begin{pmatrix} 0 & -2 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix}. \ \square$$

6 Using Zorn's Lemma, prove that in each commutative ring with identity, minimal prime ideals exist.

Proof: See **First Year Pool, Exercise 50**.

7 Let G be a group of 395 elements. Prove that the Sylow 11-subgroups are normal and that any Sylow 7-subgroup lies in the center.

Proof: See **First Year Pool, Exercise 44**.

8 Let p be prime and let Z_{p^2} be the cyclic group of order p^2. Prove that the automorphism group of Z_{p^2} is cyclic.

Proof:

Firstly, the automorphism group of Z_{p^2} has $p^2 - p = p(p-1)$ elements since $\varphi(p^2) = p(p-1)$, where φ is the Euler totient function. Let P be the Sylow p-subgroup of $\mathrm{Aut}(Z_{p^2})$. Clearly, $|P| = p$, and so P is cyclic. Consider the ring homomorphism $\psi : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $a+(p^2) \mapsto a+(p)$ which is reduction modulo p. This map gives a surjective group homomorphism from $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ to $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (as it's the multiplicative group of a finite field). The kernel of this map has order p and so any Sylow q-subgroup of $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ with $q \neq p$ must be isomorphic to a subgroup of $\mathbb{Z}/p\mathbb{Z}$. Since every subgroup of a cyclic group is cyclic, we have that all Sylow subgroups of $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ are cyclic. Therefore (why?) $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ itself is cyclic. □

9 Let R be a ring with identity and M be an R-module. An element $x \in M$ is called a *torsion element* if $rx = 0$ for some nonzero $r \in R$. Let $T(M)$ denote the subset of all torsion elements of M.

(a) If R is an integral domain, show that $T(M)$ is a submodule of M.

(b) Give an example to show that $T(M)$ in general is not a submodule of M.

Proof: See **First Year Pool, Exercise 72**.

10 Suppose that V is a finite dimensional vector space over the field F and that $T : V \to W$ is a linear transformation into a vector space W over F. Prove that $\dim(V) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T))$. (Caution: The finite dimensionality of $\mathrm{Im}(T)$ must be established.)

Proof: See **First Year Pool, Exercise 80**.

4.4 May 1998

1 (a) State the class equation for finite groups.

(b) Prove that a group of prime order power p^a with $a > 1$ has a nontrivial center.

(c) Hence or otherwise prove that such a group has normal subgroups of orders p^b for all $0 \leq b \leq a$. (Hint: Factor out a normal subgroup and use induction.)

Proof:

Let G be a finite group and let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center of G. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \big[G : C_G(g_i)\big].$$

For a proof that p-groups have nontrivial center, see **First Year Pool, Exercise 6**.

We proceed by induction on a. If $a = 1$, then the theorem follows trivially. Now, let G be a group of order p^a with $a > 1$. Let b be such that $0 \leq b \leq a$. If $b = 0$, then the theorem holds, so let $b > 0$. We wish to show that G has a normal subgroup of order p^b. Since $Z(G)$ is nontrivial, we can apply Cauchy's Theorem to $Z(G)$ to find an element of order p and a subgroup H of $Z(G)$ which is generated by p. So, $|H| = p$ and $H \trianglelefteq G$. Consider the group G/H which has order $p^a/p = p^{a-1}$. By induction, G/H has a normal subgroup P of order p^{b-1}. By the lattice isomorphism theorem, the preimage of P in G is normal in G and has order $p^{b-1} \cdot p = p^b$, which is the subgroup we're looking for. □

2 Let F be a field.

(a) Define the *minimal polynomial* of an element in some extension field of F, and the *minimal polynomial* of a linear transformation of a finite-dimensional vector space over F.

(b) Show that the former must always be irreducible, but the latter need not be.

Proof:

The minimal polynomial of an element α which is algebraic over the field F is the unique monic polynomial of least degree $m_\alpha(x) \in F[x]$ such that $m_\alpha(\alpha) = 0_F$.

Let V be a finite-dimensional vector space over F and let T be a linear transformation on V. Treating V as an $F[x]$ module via T, the minimal polynomial of T is the unique monic polynomial which generates the ideal $\text{Ann}(V)$ (i.e., the annihilator of V) in $F[x]$.

Let α be an algebraic element over the field F and consider the minimal polynomial of α over F, denotes $m_\alpha(x)$. Suppose toward a contradiction that $m_\alpha(x)$ factored into $m_\alpha(x) = f(x)g(x)$ with $\deg(f(x)) > 1$ and $\deg(g(x)) > 0$. Then, $f(\alpha)g(\alpha) = 0$ and since fields are integral domains, we have that either $f(\alpha) = 0$ or $g(\alpha) = 0$. Hence, $m_\alpha(x)$ cannot be a polynomial with least degree such that $m_\alpha(\alpha) = 0$, which is a contradiction. Therefore, $m_\alpha(x)$ must be irreducible.

To see that the minimal polynomial of a linear transformation need not be irreducible, consider the invariant factor list

$$x - 1, \;\; x^2 - 1.$$

A linear transformation with this invariant factor list has rational canonical form

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

and must have minimal polynomial $x^2 - 1$ which is not irreducible. Since linear transformations represented by this invariant factor list must exist, we have shown the minimal polynomials of linear transformations need not be irreducible. □

3 (a) Using the ring of polynomials $\mathbb{F}_5[x]$ with coefficients in the field of integers mod 5, or otherwise, prove the existence of a field F of 125 elements.

(b) Show that the elements of F are precisely the roots of the polynomial $x^{125} - x \in \mathbb{F}_5[x]$.

Proof:

Consider the polynomial $p(x) := x^3 + x + 1 \in \mathbb{F}_5[x]$. If this polynomial were reducible then it must have a linear root. Observing that $p(0) = 1$, $p(1) = 3$, $p(2) = 1$, $p(3) = 1$ and $p(4) = 4$, we see that $p(x)$ is irreducible. Hence, letting u be a root of $p(x)$ we have that $\mathbb{F}_5(u) \cong \mathbb{F}_5[x]/(p(x))$, and $\left[\mathbb{F}_5(u) : \mathbb{F}_5\right]$ has degree 3. Therefore, $|\mathbb{F}_5(u)| = |\mathbb{F}_5|^3 = 5^3 = 125$, and so the existence of a field of 125 elements has been shown.

To see that this field is in fact the field of all roots of the polynomial $x^{125} - x \in \mathbb{F}_5[x]$, see **First Year Pool, Exercise 113**. □

4 Let $F \subseteq K$ be a field extension and $\alpha \in K$. Prove the equivalence of the following statements:

(a) α is algebraic over F.

(b) $F(\alpha) = F[\alpha]$.

(c) $F(\alpha)$ has finite degree over F.

Proof:

(a) $\Longrightarrow$ (b)

Let α be an algebraic element over F. Let $m(x)$ be the minimal polynomial of α over F. Note that $F[\alpha]$ is the set of all elements $f(\alpha)$ for $f \in F[x]$ and $F(\alpha)$ is the set of all elements $f(\alpha)g(\alpha)^{-1}$ for $f, g \in F[x]$.

Recall that $F[\alpha] \cong F[x]/(m(x))$. Since $m(x)$ is irreducible, the ideal $(m(x))$ is maximal and so $F[x]/(m(x))$ is a field. Thus, $F[\alpha]$ is a field. Clearly, $F(\alpha) \supset F[\alpha]$. However, $F(\alpha)$ is the smallest field containing F and α, and so $F(\alpha) = F[\alpha]$. □

(b) $\Longrightarrow$ (c)

Let $F(\alpha) = F[\alpha]$. Then, every element of $F(\alpha)$ is of the form $f(\alpha)$ for some $f \in F[x]$. Letting $m(x)$ be the minimal polynomial of α with degree n, given any $f(x) \in F[x]$ we can apply the division ring to find $q(x), r(x) \in F[x]$ such that $f(x) = q(x) \cdot m(x) + r(x)$ with $\deg(r(x)) < \deg(m(x))$. Hence, $f(\alpha) = r(\alpha)$, and so the element $f(\alpha) \in F(\alpha)$ can be written as a linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Thus this set is a basis for $F(\alpha)$ over F and so $F(\alpha)$ has finite degree n over F. □

(c) $\Longrightarrow$ (a)

Let α be transcendental over F. Then, it's clear that $F(\alpha)$ is not finite dimensional over F, because there cannot be a finite basis for $F(\alpha)$ over F. This is the contrapositive of the statement to be shown. □

5 (a) Prove that every ideal in a Euclidean ring is principal.

(b) Give an example of an ideal in a unique factorization domain which is not principal. Justify your answer.

Proof:

For the proof that every Euclidean Domain is a Principal Ideal Domain, see **Important Theorems - Rings**. For an example of an Unique Factorization Domain which is not a Principal Ideal Domain, see **Popular Examples & Counterexamples - Rings**.

6 Find one representative of each conjugacy class of elements of order 3 in the group $GL_5(\mathbb{F}_3)$ of invertible 5×5 matrices with entries in the field of integers modulo 3. Hint: $x^3 - 1 = (x-1)^3$.

Proof:

Let A be an element of order 3. Then, $A^3 - I = 0$ and $A - I \neq 0$. Thus, if $m(x)$ is the minimal polynomial of A, we have that $m(x) \mid (x-1)^3$ and $m(x) \nmid (x-1)$. So, the possibilities for $m(x)$ are $(x-1)^3$ and $(x-1)^2$.

From this, the possible invariant factor lists are

$$(x-1)^3, \ \ (x-1)^2,$$

$$(x-1)^3,\ \ x-1,\ \ x-1,$$
$$(x-1)^2,\ \ (x-1)^2,\ \ x-1,$$
$$(x-1)^2,\ \ x-1,\ \ x-1,\ \ x-1.$$

The rational canonical forms corresponding to these invariant factor lists are:

$$\left(\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\ \begin{pmatrix}0&2\\1&2\end{pmatrix}\right),\quad \left(\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\ (2),\ (2)\right),$$

$$\left(\begin{pmatrix}0&2\\1&2\end{pmatrix},\ \begin{pmatrix}0&2\\1&2\end{pmatrix},\ (2)\right),\quad \left(\begin{pmatrix}0&2\\1&2\end{pmatrix},\ (2),\ (2),\ (2)\right).\ \square$$

7 Let R be a ring with unity, M a (unital) left R-module and $E(M)$ the set of R-module homomorphisms from M to M.

(a) Show how to give $E(M)$ the structure of a ring in which multiplication is composition of homomorphisms.

(b) Prove Schur's Lemma: If $M \neq 0$ and has no submodules other than $\{0\}$ and M, then $E(M)$ is a division ring.

Proof:

Let $\varphi, \psi \in E(M)$. Then, define $(\varphi+\psi)(m) := \varphi(m)+\psi(m)$ and $\varphi \cdot \psi = \varphi \circ \psi$. Since the sum of two module endomorphisms is a module endomorphism, $E(M)$ is closed under addition (in fact, the set under addition is an abelian group). Additionally, if $r \in R$ and $x, y \in M$, we have that

$$\begin{aligned}(\varphi\circ\psi)(rx+y) &= \varphi(\psi(rx+y)\\ &= \varphi(r\psi(x)+\psi(y))\\ &= r\varphi(\psi(x))+\varphi(\psi(y))\\ &= r(\varphi\circ\psi)(x)+(\varphi\circ\psi)(y).\end{aligned}$$

Thus, the composition of two module endomorphisms is a module endomorphism. Since function composition is associative, this multiplicative operation is associative. Lastly, if $\varphi \in E(M)$ and 1 is the identity function (which is in $E(M)$), we have that $\varphi \circ 1 = 1 \circ \varphi = \varphi$. So, $E(M)$ is a ring.

For the proof that $E(M)$ is a division ring, see **First Year Pool, Exercise 83**. $\square$

8 (a) Prove that a group of order 1998 has a normal subgroup of order 37 and another normal subgroup of index 2.

(b) Show further that any such group has an element of order 111.

Proof:

Let G be a group of order $1998 = 2 \cdot 3^3 \cdot 37$. Let n_{37} be the number of Sylow 37-subgroups. By **Sylow's Theorems**, $n_{37} \equiv 1 \pmod{37}$ and $n_{37} \mid 2 \cdot 3^3 = 54$. Thus, $n_{37} = 1$ and so there is one Sylow 37-subgroup P which is normal in G.

Let Q be the Sylow 3-subgroup of G, which has order 3^3. Now, the subgroup $PQ := \{pq \mid p \in P,\ q \in Q\}$ (which is a subgroup because P is normal) of G must have order $3^3 \cdot 37$ since $P \cap Q$ is trivial. So, PQ has index 2. Since all subgroups of index 2 are normal, PQ is normal.

Now we need find an element of order $111 = 3 \cdot 37$. Since P is cyclic it is generated by some element p of order 37. By **Cauchy's Theorem** there is an element q of order 3. (Now what?)

9 (Incomplete) Show that the ring of $n \times n$ matrices over a field has no two-sided ideals others than the zero ideal and the ring itself. Exhibit a nonzero proper, left ideal of this ring.

Proof: (Incomplete)

10 State and prove Cayley's Theorem about finite groups.

Proof: See **First Year Pool, Exercise 1**.

Index