Contents

1 Introduction

This document contains solutions to questions that have appeared on UCSB's Algebra Qualifying Exams. Some solutions are my own, some are inspired by Kyle Hansen and Zach Wagner's solutions, and others are inspired by Jacob Yakimov's solutions. Please email me with errors/corrections if you notice anything that should be changed.

The solutions are organized based on the topics addressed in the question. The problems statements also indicate which qualifying exams the problem has appeared. For ease of access, Section 2 lists the problems by qualifying exam.

2 Directory

- **Fall 2021**:
  - G1 Problem 4.29
  - G2 Problem 4.3
  - G3 Problem 4.12
- **Fall 2020**:
  - G1 Problem 7.29
  - G2 Problem 4.21
  - G3 Problem 7.26
  - RF1 Problem 5.12
  - RF2 Problem 7.31
  - RF3 Problem 7.32
  - LA1 Problem 7.33
  - LA2 Problem 6.11
  - LA3 Problem 7.34
- **Spring 2020**:
  - G3 Problem 4.5
  - RF3 Problem 5.16
  - RF4 Problem 5.11
  - LA3 Problem 6.6
- **Fall 2019**: RF1 Problem 5.6
- **Spring 2019**:
  - G1 Problem 4.10
  - G1 Problem 4.23
  - LA1 Problem 6.1
  - LA2 Problem 6.18
  - LA3 Problem **??**
  - LA4 Problem 6.15
- **Fall 2018**:
  - G1 Problem 4.33
  - G2 Problem 4.13
  - G3 Problem 4.35
  - RF1 Problem 5.15
- **Spring 2018**:
  - G1 Problem 4.25
  - G2 Problem 4.15
  - G3 Problem 4.31
  - RF1 Problem 5.5

  - RF3 Problem 5.21
  - LA1 Problem **??**
  - LA2 Problem 6.14

- **Fall 2017**:
  - G1 Problem 4.24
  - G2 Problem 4.6
  - G3 Problem **??**
  - RF2 Problem 5.19
  - RF3 Problem 5.2
  - LA2 Problem 6.2

- **Fall 2016**:
  - G1 Problem 4.26
  - G2 Problem 4.2
  - G3 Problem 4.19
  - RF3 Problem 5.4
  - LA1 Problem 6.8

- **Spring 2016**:
  - G1 Problem 4.7

- **Fall 2012**:
  - G1 Problem 4.17
  - G2 Problem 4.32, Problem 4.27
  - G3 Problem 4.10
  - RF1 Problem 7.10
  - RF2 Problem 7.11
  - RF3 Problem 5.10
  - LA1 Problem 6.16
  - LA2 Problem 6.9
  - LA3 Problem 7.12

- **Fall 2014**:
  - G1 Problem 4.19
  - G2 Problem 5.16
  - G3 Problem 4.16
  - RF1 Problem **??**
  - RF2 Problem 5.20
  - RF3 Problem 5.9
  - LA1 Problem 6.8
  - LA2 Problem 6.12
  - LA3 Problem 6.17

- **Fall 2013**:

  - G1 Problem 4.11
  - G2 Problem 4.34
  - G3 Problem 7.19
  - RF1 Problem 7.20
  - RF2 Problem 7.21
  - RF3 Problem 7.22
  - LA1 Problem 6.2
  - LA2 Problem 7.23
  - LA3 Problem 7.24
- **Spring 2013**:
  - G1 Problem 7.1
  - G2 Problem 7.2
  - G3 Problem 7.3
  - RF1 Problem 7.4
  - RF2 Problem 7.5
  - RF3 Problem 7.6
  - LA1 Problem 7.7
  - LA2 Problem 7.8
  - LA3 Problem 7.9
- **Spring 2012**:
  - G1 Problem 4.9
  - G2 Problem 4.8
  - G3 Problem 7.13
  - RF1 Problem 7.14
  - RF2 Problem 7.15
  - RF3 Problem 7.16
  - LA1 Problem 7.17
  - LA2 Problem 6.4
  - LA3 Problem 7.18
- **Spring 2011**:
  - RF2 Problem 5.7
  - RF3 Problem 5.21
- **Fall 2004**:
  - G1 Problem 4.1
  - RF1 Problem 5.17
  - L1 Problem 6.10
  - L2 Problem 6.13
- **Spring 2004**
  - G1 Problem 4.29

  - RF1 Problem **??**, part (c) still needs to be solved

- **Spring 2003**
  - G1 Problem 4.11
  - G2 Problem 4.34
  - RF1 Problem 5.1
  - RF2 Problem 5.19
  - RF3 Problem 5.2
  - L1 Problem **??**

- **Fall 2003**:
  - G1 Problem 4.30
  - G2 Problem 4.4
  - G3 Problem 4.35
  - RF1 Problem 5.13
  - RF3 Problem 5.18

3 Results to Memorize

3.1 Common Linear Algebra Results

Proposition 3.1: Eigenvectors of Distinct Eigenvalues are Linearly Independent

Let $T \in \mathscr{L}(V)$ and suppose that $\lambda_1, \ldots, \lambda_m$ are distinct eigenvalues of T and $v_1, \ldots, v_m$ are the corresponding eigenvectors. Then, $v_1, \ldots, v_m$ is linearly independent.

Proof. Assume that $v_1, \ldots, v_m$ are linearly dependent. Then there exists some minimal index k for which $v_k \in \text{span}\{\text{v}_1, \ldots, \text{v}_\text{m}\}$. That is,

$$v_k = a_1 v_1 + \cdots + a_{k-1} v_{k-1} \tag{1}$$

and by the minimality of k, $a_{k-1} \neq 0$. Applying T to both sides of (1) yields

$$Tv_k = \sum_{j=1}^{k-1} a_j T v_j \tag{2}$$

which is the same as

$$\lambda_k v_k = \sum_{j=1}^{k-1} a_j \lambda_j v_j. \tag{3}$$

On the other hand, multiplying both sides of (1) by λ_k yields

$$\lambda_k v_k = \sum_{j=1}^{k-1} a_j \lambda_k v_j. \tag{4}$$

Then, subtracting (3) from (4) yields

$$0 = (\lambda_k - \lambda_1) a_1 v_1 + \cdots + (\lambda_k - \lambda_{k-1}) a_{k-1} v_{k-1}.$$

But $v_1, \ldots, v_{k-1}$ are linearly independent and therefore each $(\lambda_k - \lambda_j) a_j = 0$. As $\lambda_k \neq \lambda_j$, it must be the case that each $a_j = 0$, a contradiction. □

Proposition 3.2: Every Complex Operator has an Eigenvalue

Suppose that V is a finite dimensional complex vector space and $T \in \mathscr{L}(V)$. Then T has an eigenvalue.

Proof. Suppose that $\dim(V) = n$ and $v \in V$ is nonzero. Consider the collection of vectors $v, Tv, \ldots, T^n v$. Since this is a collection of $n+1$ vectors in an n-dimensional space, the collection must be linearly dependent. Therefore there exist $a_0, \ldots, a_n \in \mathbb{C}$, not all zero, such that

$$0 = a_0 v + a_1 T v + \cdots + a_n T^n v.$$

If $a_1 = \cdots = a_n = 0$, then $a_0 = 0$ since $v \neq 0$. Therefore not all of $a_1, \ldots, a_k$ can be zero. Define a polynomial $f \in \mathbb{C}[z]$ by

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n.$$

Then f splits over $\mathbb{C}$ into a polynomial of the form

$$f(z) = c(z - \lambda_1) \cdots (z - \lambda_m)$$

with each $\lambda_j \in \mathbb{C}$ and $c \in \mathbb{C}$ is nonzero. Therefore,

$$\begin{aligned} 0 &= a_0 v + a_1 Tv + \cdots + a_n T^n v \\ &= (a_0 I + a_1 T + \cdots + a_n T^n)v \\ &= c(T - \lambda_1 I) \cdots (T - \lambda_m I)v \end{aligned}$$

This means that $v \in (T - \lambda_j I)$ for some j. Since $v \neq 0$, this means that some $T - \lambda_j I$ is not injective, meaning that λ_j is an eigenvalue. □

Proposition 3.3: Every Complex Operator has some Upper-Triangular Matrix

Suppose that V is a finite dimensional complex vector space and $T \in \mathscr{L}(V)$. Then T has an upper-triangular matrix with respect to some basis of V.

Proof. We proceed by induction on the dimension of V. If $\dim(V) = 1$, any matrix for T is trivially upper triangular. Assume now that $\dim(V) > 0$ and that the result holds over any vector space with dimension less than $\dim(V)$. From 3.2, there exists some eigenvalue λ of T. Define $U = \text{range}(T - \lambda I)$. Since λ is an eigenvalue, $T - \lambda I$ is not surjective and thus $\dim(U) < \dim(V)$.

For any $u \in U$,

$$Tu = (T - \lambda I)u + \lambda u$$

is the sum of two vectors in U and thus is in U itself. This means that $T|_U \in \mathscr{L}(U)$. By the inductive hypothesis, there exists a basis $\{u_1, \ldots, u_m\}$ of U with respect to which the matrix of $T|_U$ is upper-triangular. Notice that for each j,

$$Tu_j = T|_U u_j \in \text{span}\{\text{u}_1, \ldots, \text{u}_\text{j}\}$$

where the second equality follows from the fact that the matrix of $T|_U$ is upper-triangular. Extend the basis for U to a basis $\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$. For each v_k,

$$Tv_k = (T - \lambda I)v_k + \lambda v_k.$$

Then, $(T - \lambda I)v_k \in U$ meaning that it may be written as a linear combination of $\{u_1, \ldots, u_m\}$. This means that $Tv_k \in \text{span}\{\text{u}_1, \ldots, \text{u}_\text{m}, \text{v}_1, \ldots, \text{v}_\text{k}\}$. With respect to this chosen basis, the matrix of T is thus upper-triangular. □

4 Groups

4.1 Properties of Normal Subgroups

Problem 4.1: (F04.G1)

Prove that if H and K are normal subgroups of a group G and $HK = G$ then

$$G/(H \cap K) \cong (G/H) \times (G/K).$$

Proof. Define a map $\varphi : G/(H \cap K) \to (G/H) \times (G/K)$ by

$$\varphi(g) = (gH, gK).$$

For any $a, b \in G$,

$$\varphi(ab) = (abH, abK) = (aH, aK) \cdot (bH, bK)$$

following directly from the definition of multiplication in the quotient group and in a direct product. Therefore, φ is a homomorphism.

To see that φ is surjective, consider an arbitrary element $(aH, bK) \in G/H \times G/K$. Because $G = HK$, write

$$a = h_1 k_1$$

and

$$b = h_2 k_2$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Consider the element $g = k_1 h_2 \in G$.

Because H is normal in G, $k_1^{-1} h_1 k_1 \in H$ and therefore $h_2^{-1} k_1^{-1} h_1 k_1 \in H$. This implies that

$$gH = k_1 h_2 h_2^{-1} k_1^{-1} h_1 k_1 H = h_1 k_1 H.$$

Similarly, since K is normal in G, $h_2^{-1} k_1^{-1} h_2 k_2 \in K$. Thus,

$$gH = k_1 h_2 h_2^{-1} k_1^{-1} h_2 k_2 = h_2 k_2 K.$$

It then follows that

$$\varphi(g) = (gH, gK) = (h_1 k_1 H, h_2 k_2 K) = (aH, bK),$$

proving that φ is surjective.

If $g \in G$ is such that $\varphi(g) = (H, K)$, then $g \in H \cap K$. Similarly, if $g \in H \cap K$, then $\varphi(g) = (gH, gK) = (H, K)$. That is, $\ker(\varphi) = H \cap K$. By the First Isomorphism Theorem,

$$G/(H \cap K) \cong (G/H) \times (G/K),$$

as desired. □

Problem 4.2: F16.G2

(i) Suppose that $H \leq G$. Define the normalizer of H in G. Prove that there is a bijection between the conjugates of H in G and the left cosets of $N_G(H)$ in G.

(ii) Deduce that if a group has a subgroup of finite index greater than one, then it has a normal subgroup of finite index greater than one.

Proof. The normalizer of H in G is the largest subgroup of G in which H is normal. Let $A = \{gHg^{-1} : g \in G\}$ and $B = \{gN_G(H) : g \in G\}$. Define $f : A \to B$ by $f\left(gHg^{-1}\right) = gN_G(H)$. To see that f is well-defined, suppose that $gHg^{-1} = aHa^{-1}$. Then $a^{-1}gH(a^{-1}g)^{-1}$ implying that $a^{-1}g \in N_G(H)$. Then, $aN_G(H) = a(a^{-1}g)N_G(H) = gN_G(H)$, proving that f is well-defined. Clearly f is surjective, and if $gN_G(H) = aN_G(H)$ then □

Problem 4.3: F21.G2

(a) Let G be a finite group with H, K normal subgroups of G. Show that if $|H|$ and $|K|$ are coprime, then $ab = ba$ for every $a \in H$, $b \in K$.

(b) Let H and N be normal subgroups of a (not necessarily finite) group G. Show that if H is not contained in N and G/N is simple, then $G/N \cong H/H \cap N$.

Proof. Since $H \cap K$ is a subgroup of both H and K, Lagrange's Theorem implies that $|H \cap K|$ must divide both $|H|$ and $|K|$. This means that $|H \cap K| = 1$ and therefore $H \cap K = \{e\}$.

Let $a \in H$ and $b \in K$. As H is normal, $bHb^{-1} = H$ and in particular, $ba^{-1}b^{-1} \in H$. Since H is closed under multiplication and inverses, $aba^{-1}b^{-1} \in H$. Similarly, $aKa^{-1} = K$ implies that $aba^{-1} \in K$ and therefore $aba^{-1}b^{-1} \in K$. Thus, $aba^{-1}b^{-1} \in H \cap K$ and as the intersection is trivial it follows that $ab = ba$. □

Proof. Define a homomorphism $\varphi : H \to G/N$ by $\varphi(h) = hN$. Because H is normal, the $\varphi(H)$ must be a normal subgroup of G/N. But, H is not contained in G/N and therefore there exists some $h \in H$ where $hN \neq N$. Since G/N is simple the only normal subgroups of G/N are G/N and the trivial subgroup. Therefore, $\text{im}(\varphi) = G/N$. For any $n \in H \cap N$, $\varphi(n) = nN = N$. If $h \in H$ and $\varphi(h) = N$ then $hN = N$ implying that $h \in N$. This implies that $\ker(\varphi) = H \cap N$ and thus by the First Isomorphism Theorem,

$$G/N \cong H/H \cap N$$

□

4.2 General Group Theory

Problem 4.4: (F03.G2)

Suppose that G is a finite group and let K be a normal subgroup of G such that $|K|$ and $[G : K]$ are coprime. Show that K is the unique subgroup of order $|K|$.

Proof. Let $H \leq G$ be a subgroup such that $|H| = |K|$. Because K is normal, HK is a subgroup of G. Lagrange's Theorem implies that $|HK|$ divides $|G|$. Notice that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

and

$$|G| = |K| \cdot [G : K].$$

Therefore, $\frac{|H| \cdot |K|}{|H \cap K|}$ divides $|K| \cdot [G : K]$. By dividing each quantity by $|K|$, it follows that $\frac{|H|}{|H \cap K|}$ divides $[G : K]$. That is, there exists $n \in \mathbb{N}$ such that

$$n\frac{|H|}{|H \cap K|} = [G : K].$$

Multiplying both sides by $|H \cap K|$,

$$n \cdot |H| = |H \cap K| \cdot [G : K]$$

meaning that $|H|$ divides $|H \cap K| \cdot [G : K]$. But, $|H|$ and $[G : K]$ are coprime and therefore $|H|$ divides $|H \cap K|$. This implies that $H = H \cap K$ and so $H = K$. □

Problem 4.5: (S20.G3)

(a) Prove that the centralizer of an element is a subgroup.

(b) If G is a finite group, prove that the number of elements in the conjugacy class divides the order of G.

Proof. Let $a \in G$ and let $C_G(a)$ denote the centralizer of a. If e is the identity element in G, then $ea = ae$ and so $e \in C_G(a)$. Suppose now that $g, h \in C_G(a)$. Then, $ga = ag$ and $ha = ah$. Therefore, $(gh)a = g(ah) = a(gh)$ proving that $C_G(a)$ is closed under multiplication. Multiplying $ga = ag$ by g^{-1} on the left and right of each side of the equation shows that $g^{-1} \in C_G(a)$ and so $C_G(a)$ is closed under inverses. □

Proof. Let $a \in G$ and let Cl(a) denote the conjugacy class of a. Define $f : \{xC_G(a)\} \to \text{Cl(a)}$ by $f : xC_G(a) \mapsto xax^{-1}$. To see that f is well-defined, suppose that $xC_G(a) = yC_G(a)$. Then $x = yg$ for some $g \in C_G(a)$. This means that g and g^{-1} commute with a. Therefore,

$$xax^{-1} = (yg)a(yg)^{-1} = ygag^{-1}y^{-1} = yay^{-1}$$

and so f is well-defined. Clearly f is surjective. Now suppose that $xax^{-1} = yay^{-1}$. Then, $e = (x^{-1}y)a(x^{-1}y)^{-1}a^{-1}$ meaning that $x^{-1}y \in C_G(a)$. That is, $xC_G(a) = yC_G(a)$.

Since f is a bijection, the size of Cl(a) is equal to the number of left cosets of $C_G(a)$ in G and therefore divides $|G|$, as desired. □

Problem 4.6: (F17.G2)

(i) Let G be a finite group and H a subgroup of G. Prove that the order of H divides the order of G.

(ii) Let $\mathbb{C}^*$ be the multiplicative group of nonzero complex numbers. If H is a subgroup of $\mathbb{C}^*$ of finite index, prove that $H = \mathbb{C}^*$.

Proof. This is an immediate consequence of Lagrange's Theorem. See 4.10. □

Proof. Let $H \leq \mathbb{C}^*$ and suppose that $[\mathbb{C}^* : H] = m$. Let $z \in \mathbb{C}$ be arbitrary. Then,

$$z^m H = (zH)^m = H$$

implying that $z^m \in H$. Now let $\omega \in \mathbb{C}^*$ be arbitrary and consider the polynomial $x^m - \omega$ over $\mathbb{C}$. This polynomial has some root, say $z \in \mathbb{C}^*$. This means that $z^m - \omega = 0$ or equivalently, $\omega = z^m$. But, $z^m \in H$ and so $\omega \in H$. Since ω was arbitrary, $\mathbb{C}^* = H$. □

Problem 4.7: (S16.G1)

Explicitly describe two non-isomorphic, nonabelian groups of order 12.

Proof. Consider A_4 and D_{12}. Both groups are of order 12. However, D_{12} contains an element of order 6 and

A_4 does not. To see this, consider the elements in A_4:

$$\begin{array}{l}(1)\\(1\quad 2)(3\quad 4)\\(1\quad 3)(2\quad 4)\\(1\quad 4)(2\quad 3)\\(1\quad 2\quad 3)\\(1\quad 3\quad 2)\\(1\quad 2\quad 4)\\(1\quad 4\quad 2)\\(1\quad 3\quad 4)\\(1\quad 4\quad 3)\\(2\quad 3\quad 4)\\(2\quad 4\quad 3)\end{array}$$

Upon inspection, every element in A_4 is of order 1,2, or 3. In particular, there are no elements of order 6. □

Problem 4.8: (S12.G2)

(a) State (any version of) the Fundamental Theorem of finite abelian groups.

(b) Classify all abelian groups of order 144.

(c) Explain which group in part (b) is isomorphic to the group $\mathbb{Z}_4 \times \mathbb{Z}_{36}$.

Suppose that G is a finite abelian group. Then G is isomorphic to a direct sum of the form

$$\bigoplus_{i=1}^{m} \mathbb{Z}_{k_i}$$

where each k_i is a power of some prime and $\prod_{i=1}^{m} k_i = |G|$. Note that the k_i need not be powers of distinct primes.

Solution. Observe that $144 = 2^4 \cdot 3$. Therefore, the following are the abelian groups of order 144, up to isomorphism:

$$\begin{aligned}\mathbb{Z}_{16} \times \mathbb{Z}_9\\ \mathbb{Z}_{16} \times \mathbb{Z}_3^2\\ \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_9\\ \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3^2\\ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9\\ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2\\ \mathbb{Z}_4 \times \mathbb{Z}_2^2 \times \mathbb{Z}_9\\ \mathbb{Z}_4 \times \mathbb{Z}_2^2 \times \mathbb{Z}_3^2\\ \mathbb{Z}_2^4 \times \mathbb{Z}_9\\ \mathbb{Z}_2^4 \times \mathbb{Z}_3^2\end{aligned}$$

The group $\mathbb{Z}_4 \times \mathbb{Z}_{36}$ is isomorphic to the group $\mathbb{Z}_4 \times Z_4 \times Z_9$. To see this, let $G = \mathbb{Z}_4 \times \mathbb{Z}_{36}$ and $H = \mathbb{Z}_4 \times \mathbb{Z}_4 \times Z_9$ and consider the homomorphism $\varphi : H \to G$ given by

$$\varphi(x, y, z) = (x, yz).$$

Clearly φ is a homomorphism and is well-defined as $yz \in \{0, 1, \ldots, 35\}$. The inverse of φ is given by $(a, b) \mapsto (a, b \bmod(4), b \bmod(9))$ since 4 and 9 are relatively prime.

Problem 4.9: S12.G1

Prove that there are at least two non-isomorphic non-abelian groups of order 24.

Proof. Consider the groups $H = D_{24}$ and $G = \mathbb{Z}_2 \times D_{12}$. Since any dihedral group is nonabelian, both H and G must be nonabelian. However, H contains an element of order 12. The order of an element $(x, y) \in G$ is the least common multiple of the order of $x \in \mathbb{Z}_2$ and $y \in D_{12}$. The highest order of an element in $\mathbb{Z}_2$ is 2 and the highest order of an element in D_{12} is 6. Since the least common multiple of 2 and 6 is 6, it is impossible for G to contain an element of order 12. □

Problem 4.10: (F19.G1, F18.G2, F17.2, F12.G3)

(a) State and prove Lagrange's Theorem.

(b) Prove that a subgroup of a cyclic group is cyclic.

Lagrange's Theorem States the following: If G is a finite group and H is a subgroup of G then $[G : H] \cdot |H| = |G|$ where $[G : H]$ is the number of distinct left cosets of H in G.

Proof. Suppose that G is a finite group and $H \leq G$ is a subgroup.

Claim: The set of left cosets of H in G partitions G.

Proof. Note that any $g \in G$ is in the coset gH since $g = g \cdot e$ where $e \in H$ is the identity element of the group. That is, each element of G is in some left coset of H.

Let $a, b \in G$ and suppose that $aH \cap bH \neq \varnothing$. Let $y \in aH \cap bH$ with $y = ah_1 = bh_2$ where $h_1, h_2 \in H$. Observe that $a = bh_1h_2^{-1}$ and $b = ah_2h_1^{-1}$. Then, for any $h \in H$,

$$ah = bh_1h_2^{-1}h \in bH$$

and

$$bh = ah_2h_1^{-1}h \in aH.$$

Therefore, $aH = bH$. Since any pair of left cosets are either disjoint or equal, it follows that the set of left cosets partitions G.

Claim: For any $g \in G$, $|H| = |gH|$.

Proof. Define $\varphi : H \to gH$ by $\varphi(h) = gh$. Clearly φ is surjective. If $gh = gh'$, multiplying each side by g^{-1} implies that $h = h'$ and so φ is injective. As φ is a bijection between H and gH, $|H| = |gH|$ as desired.

As G is finite, there are a finite number of left cosets of H in G. Let $g_1H, \ldots, g_nH$ be the left cosets of H in G. Each g_iH has $|H|$ elements and each $g \in G$ is in some g_iH. Therefore,

$$|G| = n|H| = [G : H]|H|,$$

as desired. □

Proof. Suppose that G is a cylic group and $H \leq G$ a subgroup. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. If H is the trivial subgroup, then H is generated by the identity. Otherwise, there exists $m \in \mathbb{N}$ such that $a^m \in H$ with $a^m \neq e$. Assume that m is the least such positive integer. For any $b \in H$, there exists $n \in \mathbb{N}$ such that $b = a^n$ since $b \in G$. By the Division Algorithm, there exist integers $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $n = mq + r$. Then,

$$b = a^n = a^{mq+r} = a^{mq}a^r.$$

Since $a^m \in H$, any power of a^m is also contained in H. In particular, $a^{mq}, (a^{mq})^{-1} \in H$. Therefore,

$$a^r = b\,(a^{mq})^{-1} \in H.$$

Because $0 \leq r < m$ and m is the minimal positive integer where $a^m \in H$, it follows that $r = 0$. Therefore, $n = mq$. This means that $b = a^n = a^{mq} = (a^m)^q$. Because b was arbitrary, $H = \langle a^m \rangle$ proving that H is cyclic. □

Problem 4.11: (F13.G1, S03.G1)

A subgroup H of a group G is *characteristic* if $\alpha(H) = H$ for any automorphism α of H.

(a) Prove that if H is characteristic in K and K is characteristic in G, then H is characteristic in G.

(b) Suppose now that H, K, and G are groups with H a normal subgroup of K and K a normal subgroup of G. Does this imply that H is a normal subgroup of G?

Proof. Let φ be an automorphism of G. Because K is characteristic in G, $\varphi(K) = K$. Therefore, φ restricts to an automorphism of K. Since H is characteristic in K, $\varphi(H) = H$. But since φ was an arbitrary automorphism of G, this means that H is characteristic in G. □

Solution. This need not be true. Let $G = S_4$, $H = \langle (12)(34), e \rangle$, $K = \langle (12)(34), (13)(24), (14)(23), e \rangle$. Upon inspection, H is normal in K, K is normal in G, but H is not normal in G.

4.3 The Sylow Theorems

Problem 4.12: (F21.G3)

Let p and q be distinct odd primes. Use the Sylow Theorems to show that every group of order p^2q^2 is not simple.

Proof. Suppose that $|G| = p^2q^2$ and without loss of generality, assume that $p < q$. Note that each Sylow p-subgroup is of order p^2 and each Sylow q-subgroup is of order q^2. Furthermore, the number of Sylow-p subgroups is $n_p = 1, q, q^2$ and the number of Sylow-q subgroups is $n_q = 1, p^2$. If $n_q = 1$, then the Sylow-q subgroup is normal in G and thus G is not simple. Suppose instead that $n_q = p^2$.

If Q_i, Q_j are any two distinct Sylow-q subgroups, the intersection $Q_i \cap Q_j$ is either of size 1 or q. If every pairwise intersection between the Sylow-q subgroups is trivial, then the p^2 Sylow-q subgroups account for $p^2q^2 - (p^2 - 1)$ elements implying that $n_p = 1$. That is, the Sylow-p subgroup is normal and therefore G is not simple. Suppose that some Sylow-q subgroups Q_1, Q_2 have intersection of size q. Let $N = Q_1 \cap Q_2$ and let M be the subgroup of G generated by Q_1 and Q_2. Then, $|M| > |Q_1| = q^2$ and $|M|$ divides $|G| = p^2q^2$. Therefore $|M| = pq^2$ or $|M| = p^2q^2$.
Note first that any group of prime squared order is abelian. Therefore both Q_1 and Q_2 are abelian and so $N = Q_1 \cap Q_2$ is normal in M. If $|M| = p^2q^2$ then $M = G$ and thus N is a normal subgroup of G and is nontrivial.

Now suppose that $|M| = pq^2$. I'm not sure where to go from here... Need to use this to construct a normal subgroup of G. □

Problem 4.13: F18.G2

(a) State and prove Lagrange's Theorem.

(b) Suppose that p and q are distinct primes. Prove that a nonabelian group of order pq has trivial center.

Proof. See 4.10. □

Proof. Suppose that $\mathbb{Z}(G)$ is of order q. Then $G/Z(G)$ is of order q. Any group of prime order is cyclic. But, $G/Z(G)$ cyclic implies that G is abelian (4.29), a contradiction. Therefore $|Z(G)| \neq p$ and similarly, $|Z(G)| \neq q$. As G is nonabelian, $|Z(G)| < |G|$ and by Lagrange's Theorem the only remaining possibility is $|Z(G)| = 1$. □

Problem 4.14: F16.G1

(i) Suppose that G has no subgroup of index 2. Prove that any subgroup of index 3 is normal.

(ii) Let G be the finite simple group of order 168. Prove that G is a subgroup of the alternating group on 8 letters.

Proof. Suppose that $H \subseteq G$ is of index 3. Let G act on the left cosets of H and suppose that $\varphi : G \hookrightarrow S_3$ is the permutation associated with this action. Note that φ is nontrivial. Define $K = \ker(\varphi)$. For any $a \in K$, $aH = a \cdot H = H$. Therefore, $K \subseteq H$. By the First Isomorphism Theorem,

$$G/K \cong \varphi(G) \leq S_3$$

meaning that $[G : K]$ must divide $|S_3| = 6$. By assumption, $[G : H] = 3$ and since $K \subseteq H$, $[G : K] \geq [G : H]$. This means that either $[G : K] = 3$ or $[G : K] = 6$.

If $[G : K] = 6$, then $G/K \cong S_3$. Notice that $A_3 \triangleleft S_3$ is a subgroup of index 2. Therefore, there exists a subgroup $J/K \subseteq G/K$ of index 2. However, this would imply that

$$[G : J] = [G/K : J/K] = 2,$$

contradicting the fact that G has no subgroups of index 2.

Since $[G : K] \neq 6$, it must be the case that $[G : K] = 3$. Since $K \subseteq H$ and $[G : H] = 3$, it follows that $H = K$ and thus H must be normal. □

Proof. Notice that $168 = 2^3 \cdot 3 \cdot 7$. Because G is simple, $n_7 \neq 1$ and by the Sylow Theorems, the only other possibility is that $n_7 = 8$. Let $\varphi : G \hookrightarrow S_8$ be the permutation associated with G acting on the left cosets of P, a Sylow 7-subgroup. Notice that φ is a nontrivial homomorphism. We must show that $\varphi(G) = A_8$. Where to go from here? □

Problem 4.15: S18.G2

(a) Give two examples of non abelian and non-isomorphic groups of order 80.

(b) Show that a group of order 80 cannot be simple.

Proof. Let $G = D_{80}$ and $H = \mathbb{Z}_2 \times D_{40}$. Notice that G has an element of order 80. In a direct product, the order of an element (x, y) is equal to the least common multiple of the orders of x and y in their respective groups. The maximum order of an element in D_{40} is 20 and the maximum order of an element in $\mathbb{Z}_2$ is 2. Therefore the maximum order of an element in H is $\text{lcm}(2, 20) = 20$. Since it is impossible for H to have an element of order 40, $G \ncong H$. □

Proof. Notice that $80 = 2^4 \cdot 5$. By the Sylow Theorems, $n_2 = 1, 5$ and $n_5 = 1, 16$. The Sylow 2 subgroups are of order 16 and the Sylow 5 subgroups are of order 5. This means that the Sylow 5 subgroups intersect trivially. If $n_5 \neq 1$ then there are $16 \cdot 4 = 64$ elements of order 5 accounted for. This leaves room for exactly one Sylow 2 subgroup. That is $n_2 = 1$ and so the Sylow 2 subgroup is normal in G. □

Problem 4.16: F14

(a) Let $x = (12345)$ be a cyclic permutation of $\{1, 2, 3, 4, 5\}$. Find another permutation y such that $y^{-1}xy = x^2$.

(b) Determine the order of the group G generated by x and y.

(c) Show that $x^{-1}yx$ is not a power of y.

(d) Find the number of Sylow-2 subgroups of G.

Solution. If $y \in S_5$ satisfies $y^{-1}xy = x^2$, then y also must satisfy $yx^2y^{-1} = x$. That is,

$$y(13524)y^{-1} = (12345).$$

Then y must do the following:

$$\begin{aligned} 1 &\mapsto 1 \\ 2 &\mapsto 4 \\ 3 &\mapsto 2 \\ 4 &\mapsto 5 \\ 5 &\mapsto 3 \end{aligned}$$

meaning that y has cycle decomposition $y = (2453)$. Upon inspection, $y^{-1}xy = x^2$.

Solution. Let $H = \langle x \rangle$ and $K = \langle y \rangle$. Since x is a length 5 cycle, $|H| = 5$. Similarly, $|K| = 4$. Since 5 and 4 are relatively prime, $H \cap K$ is trivial and thus

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 20.$$

Since each element of HK must be in $G = \langle x, y \rangle$, $|G| \geq 20$. It remains to show that any product of powers of x and y can be written in the form $x^i y^j$ where $0 \leq i \leq 4$ and $0 \leq j \leq 3$. To do this, note that

$$xy = yx^2$$

and

$$yx = xyx^{-1}.$$

Using these identities transforms any product of the form $y^m x^n$ into one of the form $x^i y^j$. Therefore $|G| = 20$.

Proof. Notice that $K = \langle y \rangle$ is of order 4 with

$$K = \{(1), (2453), (25)(34), (2354).\}$$

Since $x^{-1}yx = (1342) \notin K$, $x^{-1}yx$ cannot be written as a power of y. If this were possible, then the order of y would be greater than 4, a contradiction. □

Solution. Since $|G| = 2^2 \cdot 5$, the number of Sylow 2 subgroups is either 1 or 5 as these are the only numbers that divide 5 and are congruent to 1 modulo 2. Since the Sylow 2 subgroups of G are of size 4 and y and $x^{-1}yx$ both generate different subgroups of order 4, there are at least two Sylow 2 subgroups. Therefore the number of the Sylow 2 subgroups is 5.

Problem 4.17: F12.G1

(a) Let G be a finite group whose order is divisible by 2. Prove that G contains an element of order two.

(b) Suppose that the order of G is even but not divisible by 4. Prove that G is not simple.

Proof. Suppose that G is finite and that 2 divides $|G|$. Then G has an even number of elements and so

$$G = \{e, x_1, \ldots, x_n\}$$

where e is the identity element and $x_1, \ldots, x_n$ are the remaining n non-identity elements of G. As the number of elements is even, n must be odd. Observe that a nonidentity element x is of order two if and only if $x = x^{-1}$. Pair each element of G with its inverse. Since e is its own inverse, it follows that each x_i is paired with some x_j. If no x_i were of order two, then each of the n remaining elements could be paired into disjoint groups of two. This is a contradiction as n is odd. Therefore some x_i is its own inverse and thus is of order two. □

Proof. Suppose that $|G|$ is even but is not divisible by 4. That is, $|G| = 2m$ with m some odd integer greater than 1. By 4.25, G has a subgroup of index 2. Since any index 2 subgroup is normal, G has a nontrivial normal subgroup and therefore is not simple. □

Problem 4.18: S20

Let p and q be primes. Prove that a group of order pq is solvable.

Proof. Suppose that p, q are prime and G is a group of order pq. If $p = q$, then G has order p^2. Then G must be abelian and is therefore solvable. Assume now that $p \neq q$. By the Sylow Theorems there exists a subgroup $P \leq G$ of order p. Since $p \neq q$ and q is prime, there is exactly one Sylow p-subgroup. Therefore, P is normal in G. Consider the sequence of normal subgroups

$$0 \triangleleft P \triangleleft G$$

and note that G/P is of order q and $P/0$ is of order p. As both of these quotients are of prime order, they are cyclic and therefore abelian. □

Problem 4.19: F19.G1, F16.G3, F14.1

(a) Suppose that G is a group with exactly two subgroups. Prove that G is finite and of prime order.

(b) Must the converse of the previous part be true?

Proof. Suppose that G is a group with exactly two subgroups. Seeking a contradiction, suppose that G is infinite and choose some non-identity element $x \in G$. If $\langle x \rangle = G$, then G is an infinite cyclic group. That is, $G \cong \mathbb{Z}$. As $\mathbb{Z}$ has infinitely many subgroups, this is a contradiction. So, there exists $y \in G - \langle x \rangle$. In this case, there are three distinct subgroups, $\{e\}, \langle x \rangle, \langle y \rangle$, again a contradiction. Therefore, G must be finite.

Let p be some prime dividing the order of G. By Cauchy's Theorem (**??**), there exists an element x of order p. As there are only two subgroups and $p > 1$, $\langle x \rangle = G$, implying that G is of prime order p. □

Proof. Suppose that G is finite and of prime order p. By Lagrange's Theorem, any subgroup of G is of order 1 or order p. The only subgroup of order 1 is the trivial subgroup and the only subgroup of order p is G. That is, G has exactly two subgroups. □

Problem 4.20: F19

Suppose that G is a finite group with exactly three conjugacy classes. Show that G is isomorphic to either S_3 or to $\mathbb{Z}/3\mathbb{Z}$.

Proof. Let $r, s, t \geq 1$ denote the sizes of the three distinct conjugacy classes. Without loss of generality, we may assume $r = 1$ as conjugacy classes partition a group and the identity element is in its own conjugacy class. Then, $|G| = 1 + s + t$. Note that the conjugacy classes of G are the same as the orbits formed by the action of G acting on itself via conjugation. Therefore, by the Orbit Stabilizer Theorem, s and t must both divide $|G|$.

If G is abelian, then $s = t = 1$ as every element is in its own conjugacy class. This means that $|G| = 3$ and therefore $G \cong \mathbb{Z}/3\mathbb{Z}$ since this is the only group of order 3.

Now assume that G is non-abelian. Then, some conjugacy class of G must be of size greater than 1. Assume that $s \geq 2$. Note that $1 + t = |G| - s$ and since s divides $|G|$, s must divide $1 + t$. Therefore, $s \leq 1 + t$. As both s and t are positive integers, this means that $s = t$ or $s = 1 + t$. If $s = t$, then $|G| = 1 + 2s$ and since s divides $|G|$, s must divide 1. This is only possible if $s = 1$. By assumption, $s \geq 2$ and therefore we may assume that $s = 1 + t$. In this case, $|G| = 2 + 2s = 2(1 + s)$. As $s \geq 2$ and s divides $|G|$, s divides 2. That is, $s = 2$ and therefore $t = 3$. Then, $|G| = 6$. As G is non-abelian, $G \cong S_3$ since this is the only non-abelian group of order 6. □

Proof. Suppose that G is finite and has exactly three conjugacy classes, of sizes r, s, t. As conjugacy classes partition a group, G is of size $r + s + t$.

If G is abelian, every conjugacy class must be of size 1. Therefore, $|G| = 3$ and thus $G \cong \mathbb{Z}/3\mathbb{Z}$.

Suppose now that G is not abelian. Without loss of generality, assume that $r = 1$ since the identity element must be in a conjugacy class of size 1. □

Problem 4.21: F20

(a) Give two examples of non-abelian groups of order 48 that are non-isomorphic.

(b) Show that a group of order 48 cannot be simple.

Proof. Let $G = D_{48}$ and $H = D_{24} \times \mathbb{Z}_2$ where D_{48} and D_{24} are the dihedral groups of orders 48 and 24, respectively. Each of G and H are of order 48 and are clearly non-abelian. However, these groups are non-isomorphic. The generating element for rotation in G has order 48. However, the highest possible order for an element in H is 24 since the order of an element $(x, y) \in H$ is the least common multiple of the order of x in D_{24} and the order of y in $\mathbb{Z}_2$. □

Proof. Let G be of order 48. Notice that $48 = 2^4 \cdot 3$. By the Sylow Theorems, the number of Sylow 2 subgroups n_2 is either 1 or 3 as it must divide 3 and be equivalent to 1 modulo 2. Similarly, the number of Sylow 3 n_3 subgroups is either 1, 4, or 16. If G is not simple than $n_2, n_3 \neq 1$ since either being equal to 1 would guarantee a normal subgroup. This means that $n_2 = 3$ and $n_3 = 4$ or $n_3 = 6$. Each Sylow 2 subgroup is of size 16. Suppose that H and K are two distinct Sylow 2 subgroups. Then, $H \cap K$ is a subgroup of H and must be of order 1,2,4, or 8. If $|H \cap K| \leq 4$, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K} \geq 64.$$

But, $HK \subseteq G$ and therefore this is impossible. Thus, $|H \cap K| = 8$. As any subgroup of index two is normal, $H \cap K$ is normal in each of H and K. The normalizer N of $H \cap K$ in G includes H, K, and $H \cap K$ and therefore must be of size at least $\text{lcm}(8, 16) = 24$. Since the normalizer is also a subgroup in G, either $|N| = 24$ or $|N| = 48$ since $|H|$ must also divide $|N|$. In either case, N is normal in G as N is either of index 2 or equal to G. This is a contradiction to G being simple. □

Problem 4.22: S19

Prove that every group of order 21 has a normal subgroup of index 3, but that not every group of order 21 is abelian.

Proof. Suppose that $|G| = 21$. By the Sylow Theorems, there exists a Sylow 7-subgroup, say P, of order 7. There's exactly one Sylow-7 subgroup because the only number that divides 1 and is equivalent to 1 modulo 7 is 1. Therefore P is normal in G and $|G/P| = 3$. □

Proof. Consider the subgroup of $M_{2\times 2}(\mathbb{Z}_7)$ given by $G = \langle A, B\rangle$ where

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

and

$$A = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}.$$

Upon inspection,

$$A^7 = B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$BAB^{-1} = A^2.$$

This group is non-abelian but is of order 21.

I should probably add more details here about why this construction is guaranteed to be of order 21. It's clear there are at most 21 elements, but how do we show that there are no duplicates? □

4.4 Permutation Groups

Problem 4.23: S19.G2

You may assume that every permutation has a cycle decomposition $\sigma = \sigma_1 \cdots \sigma_k$ where $\sigma_1, \ldots, \sigma_k$ are pairwise disjoint cycles. Prove that $\sigma, \tau \in S_n$ are conjugate in S_n if and only if for each $m \geq 2$ the number of m-cycles in a cycle decomposition of σ equals the number of m-cycles in a cycle decomposition of τ.

Proof. **Claim:** Two cycles $\sigma, \tau \in S_n$ are conjugate if and only if they are cycles of the same length.

Proof. Suppose first that $\tau = x\sigma x^{-1}$ for some $x \in S_n$. Further suppose that σ is an m-cycle and τ is a k-cycle. Since σ is an m-cycle, $\sigma^m = (1)$. Observe that

$$\tau^m = (x\sigma x^{-1})^m = x\sigma^m x^{-1} = xx^{-1} = (1).$$

This implies that the order of τ is at most m. Suppose now that $\tau^k = (1)$ for some $k < m$. Then,

$$(1) = \tau^k = (x\sigma x^{-1})^k = x\sigma^k x^{-1}.$$

Left-multiplying by x^{-1} and right-multiplying by x implies that $\sigma^k = (1)$, contradicting the minimality of m. Therefore, but σ and τ are m-cycles.

Now assume that σ and τ are both m-cycles. Write $\sigma = (k_1 \ \dots \ k_m)$ and $\tau = (\ell_1 \ \dots \ \ell_m)$ where $k_1, \dots, k_m \in \{1, \dots, n\}$ are distinct and $\ell_1, \dots, \ell_m \in \{1, \dots, n\}$ are distinct. Let $k'_1, \dots, k'_{n-m}$ and $\ell'_1, \dots, \ell'_{n-m}$ denote the elements of $\{1, \dots, n\}$ that do not appear in the cycle notation for σ and τ, respectively.

Define an element $x \in S_n$ as follows: for each k_i, let $x : k_i \mapsto \ell_i$. Note that defining x in this way is well-defined as each k_i is distinct. Similarly, for each k'_i, let $x : k'_i \mapsto \ell'_i$. It remains to show that $x\sigma x^{-1} = \tau$.

Consider any ℓ_i. By construction,

$$x\sigma x^{-1}(\ell_i) = x\sigma(k_i) = x(k_{i+1}).$$

If $i = m$, then this equality becomes

$$x\sigma x^{-1}(\ell_m) = x(k_1).$$

On the other hand,

$$\tau(\ell_i) = \ell_{i+1} = x(k_{i+1})$$

and when $i = m$,

$$\tau(\ell_m) = \ell_1 = x(k_1).$$

Note also that τ fixes each ℓ'_i. For each ℓ'_i,

$$x\sigma x^{-1}(\ell'_i) = x\sigma(k'_i) = x(k'_i) = \ell'_i$$

since σ fixes each k'_i. Adjust the equation as done previously in the case that $i = m$. This proves that $x\sigma x^{-1} = \tau$.

□

Problem 4.24: F17.G1

(i) Let G be a finite group and $H \leq G$ such that $[G : H] = n$. Prove that there is a nontrivial homomorphism $\rho : G \to S_n$ with $\ker(\rho) \leq H$.

(ii) Let G be a finite group and H a subgroup of G whose index in G is the smallest prime dividing $|G|$. Show that H is a normal subgroup of G.

Proof. Let $\rho : G \to S_n$ be the homomorphism given by G acting on the left cosets of H in G via multiplication. If $g \in \ker(\rho)$ then $g \cdot (xH) = H$ for every left coset xH. In particular, $g \cdot (H) = H$ and therefore $g \in H$. That is, $\ker(\rho) \leq H$.

Since $[G : H] > 1$, there exists some $g \in G \setminus H$. Then, $g \cdot H = gH \neq H$ and so ρ is nontrivial. □

Proof. Suppose that p is the smallest prime dividing $|G|$ and that $H \leq G$ is a subgroup such that $[G : H] = p$. From the previous proof, there exists a nontrivial homomorphism $\rho : G \to S_p$ such that $\ker(\rho) \subseteq H$. Define $K = \ker(\rho)$. By the First Isomorphism Theorem, G/K is isomorphic to some subgroup J of S_p. Then $|J|$ must divide $|S_p| = p!$ and $|J|$ must divide $|G|$. If $|G/K| = |J| = 1$, then $G = K$. Then $H = G$ and is thus trivially normal in G. Otherwise, the minimality of p implies that $|J| = p$. Then $[G : K] = p = [G : H]$ and since $K \leq H$, it follows that $H = K$, a normal subgroiup.
Since p is the smallest prime that divides □

Problem 4.25: S18.G1

Show that if G is a group of order $2k$ where k is odd, then G has a subgroup of index 2.

Proof. Enumerate the elements of G with values $\{1, \ldots, 2k\}$. For each $a \in G$, let $\varphi_a : G \to G$ be left multiplication by a. Identify φ_a with the permutation in S_{2k} corresponding to the image of φ_a. Then define $\varphi : G \to S_{2k}$ by $\varphi : a \mapsto \varphi_a \in S_{2k}$. By construction, φ is injective and a homomorphism meaning that G is isomorphic to some subgroup H of S_{2k}.

By Cauchy's Theorem (or 4.17), G has an element x of order 2 since the order of G is divisible by two. Consider $\varphi(x) \in H$. Since x is of order 2 and φ is an isomorphism, $\varphi(x)$ must also be of order 2. That is, $\varphi(x)$ is the product of some number of disjoint transpositions. Since $|G| = 2k$, there are at most k disjoint transpositions in $\varphi(x)$. If $\varphi(x)$ is the product of less than k transpositions, then there exists $g \in G$ such that $xg = g$. However, this would imply that $x = e$ which contradicts the fact that x is of order 2. Therefore $\varphi(x)$ is the product of exactly k disjoint transpositions. Since k is odd, $H \not\subseteq A_{2k}$. Let $\sigma : H \to \mathbb{Z}_2$ be the sign map. Then, $\sigma\varphi : G \to \mathbb{Z}_2$ is surjective and if $K = \ker(\sigma\varphi)$,

$$G/K \cong \mathbb{Z}_2.$$

That is, K is a normal subgroup of index 2. □

Problem 4.26: F16.G1

(i) Suppose that G has no subgroup of index 2. Prove that any subgroup of index 3 is normal.

(ii) Let G be the finite simple group of order 168. Prove that G is a subgroup of A_8.

Proof. Let $H \subseteq G$ be of index 3. Let $\varphi : G \to S_3$ be the homomorphism of the group action of G acting on the left cosets of H by $g \cdot xH = (gx)H$. Notice that φ is therefore a nontrivial homomorphism. Define $K = \ker(\varphi)$ so that K is a normal subgroup of G. We prove that $K = H$ to show that H is normal in G.

If $a \in K$, then $H = a \cdot H = aH$ implying that $a \in H$. That is, $K \subseteq H$ and so $[G : K] \geq [G : H]$. By the First Isomorphism Theorem, G/K is isomorphic to some subgroup of S_3. Since $[G : K] = |G/K|$ which must divide 6 and $[G : K] \geq [G : H] = 3$, the only possible values for $[G : K]$ are 3 or 6. If $[G : K] = 6$, then $G/K \cong S_3$ which has a normal subgroup of index 2. Then G/K must have a subgroup, say J/K, of index 2. This would then imply that $[G : J] = 2$, a contradiction. Therefore, $[G : K] = 3$ and so $H = K$. □

Proof. Notice that $168 = 2^3 \cdot 3 \cdot 7$. By the Sylow Theorems, $n_7 = 1$ or $n_7 = 8$. Since G is simple, $n_7 \neq 1$ or else G would have a nontrivial normal subgroup. Therefore $n_7 = 8$. Map G into S_8 by letting G act on the eight Sylow-7 subgroups via conjugation. Let $\varphi : G \to S_8$ be the homomorphism associated with this action. Let $\mathrm{sgn} : \mathrm{S}_8 \to \mathbb{Z}_2$ be the sign map and let $\psi = \mathrm{sgn} \circ \varphi : \mathrm{G} \to \mathbb{Z}_2$. Suppose that $\varphi(G) \not\subseteq A_8$. Then there exists some odd permutation in $\varphi(G)$ and therefore ψ is a surjection. By the First Isomorphism Theorem, this implies that $G/\ker(\psi) \cong \mathbb{Z}_2$. This is impossible since then $\ker(\psi)$ would be a nontrivial normal subgroup of G. Therefore every element in $\varphi(G)$ must be an even permutation. Again, because G has no nontrivial normal subgroups, the kernel of φ must be trivial meaning that φ is indeed an embedding. □

4.5 $G/Z(G)$ is Cyclic

Problem 4.27: F12.G2

Define the center of a group.

(a) Prove that if the order of G is p^k for some prime p then G has nontrivial center.

(b) Suppose that p and q are distinct primes. Prove that a non-abelian group of order pq has trivial center.

The center of a group G is the subgroup

$$Z(G) = \{g \in G : gx = xg \text{ for any } x \in G\}$$

Proof. See 4.32 □

Proof. Suppose that G is a non-abelian group of order pq with $p \neq q$ both prime. Because G is non-abelian and the order of a subgroup of G must divide pq, $Z(G)$ is of order 1, q, or p. If $Z(G)$ is of order p then $|G/Z(G)| = q$. Since q is prime, this means that $G/Z(G)$ is cyclic. This implies that G is abelian, a contradiction (see 4.29). Similarly, if $Z(G)$ were of order q, then $G/Z(G)$ would be cyclic which contradicts G being non-abelian. Therefore $|Z(G)| = 1$ meaning that the center is trivial. □

Problem 4.28: S20

Let G be a group and H a subgroup of G contained in the center $Z(G)$ of G such that G/H is cyclic.

(a) Show that G is abelian.

(b) Show that every group of order p^2 with p a prime is abelian. *It may be assumed that a p-group has nontrivial center.*

Proof. Suppose that $G/H = \langle gH \rangle$ for some $g \in G$. Let $a, b \in G$. By assumption, $a = g^k H$ and $b = g^m H$ for some $k, m \in \mathbb{N}$. Therefore, $a = g^k h_1$ and $b = g^m h_2$. Since elements in H commute with every element in G and powers of G commute with one another,

$$ab = g^k h_1 g^m h_2 = g^m h_2 g^k h_1 = ba$$

proving that G is abelian. □

Proof. Suppose that $|G| = p^2$ with p a prime. Because G is a p-group, it has nontrivial center and thus $|Z(g)| > 1$. By Lagrange's Theorem, $|Z(G)| = p$ or $|Z(G)| = p^2$. If $|Z(G)| = p^2$, $Z(G) = G$. If $|Z(G)| = p$, $|G/Z(G)| = p$. That is, $G/Z(G)$ is cyclic and therefore G is abelian. □

Problem 4.29: (F21.G1, S04.G1)

Let G be a finite group and let $Z(G)$ denote the center of G.

(a) Prove that if $G/Z(G)$ is cyclic then G is abelian.

(b) Does there exist a finite group H such that $|H/Z(H)| = 7$? What if $|H/Z(H)| = 6$?

Proof. This is a special case of 4.28. □

Solution. Suppose that $|H/Z(H)| = 7$. As this group is of prime order, it must be cyclic. Therefore, by the previous result, H is abelian. That is, $H = Z(H)$ which would imply that $|H/Z(H)| = 1$, a contradiction.

If $H = S_3$ then $Z(H)$ is trivial and $|H : Z(H)| = 6$.

4.6 Group Actions

Problem 4.30: (F03.G1)

Let G be a group of order 15 which acts on a set S with 7 elements. Show that the group action has a fixed point.

Proof. From the Orbit Stabilizer Theorem, each orbit of the action must divide $|G|$ and the orbits partition S. Therefore, each orbit is of size 1,3,5, or 15 and the sum of the orbits must equal 7. The possible sizes for the orbits are:

$$\{1,1,1,1,1,1,1\}, \{1,1,1,1,3\}, \{1,1,5\}, \{1,3,3\}.$$

An orbit of size 1 corresponds to a fixed point. Since any of the possibilities has an orbit of size 1, there exists a fixed point. □

Problem 4.31: (S18.G3)

(a) Let G be a finite group acting on a finite set S. Prove that the size of the orbit of a point is equal to the index of its stabilizer.

(b) Prove the class equation:
$$|G| = |Z(G)| + \sum_{g \in I} [G : C(g)]$$
where $Z(G)$ is the center of G, $C(g)$ is the centralizer of g, and I is a set with one representative from each nontrivial conjugacy class of G.

(c) Prove that every finite p-group has nontrivial center.

Proof. Let $x^G = \{g \cdot x : g \in G\}$ denote the orbit of $x \in S$. Let $G_x = \{g \in G : g \cdot x = x\}$ denote the stabilizer subgroup of x. Let A be the collection of left-cosets of G_x in G. Define $f : x^G \to A$ by $f : g \cdot x \mapsto gG_x$.

To see that f is well-defined, suppose that $g \cdot x = h \cdot x$. Then, $(h^{-1}g) \cdot x = x$ implying that $h^{-1}g \in G_x$. Therefore, $h^{-1}gG_x = G_x$ and so $gG_x = hG_x$.

Clearly f is surjective: given any $gG_x \in A$, $g \cdot x \mapsto gG_x$. If $gG_x = hG_x$, then $h^{-1}g \in G_x$ and so $(h^{-1}g) \cdot x = x$. Therefore $h \cdot x = g \cdot x$ and so f is injective.

Since f is a bijection from A to x^G,
$$|x^G| = [G : G_x].$$

□

Proof. Let G act on itself by conjugation. That is, $g \cdot x = gxg^{-1}$. Then given $x \in G$,
$$x^G = \{gxg^{-1} : g \in G\}$$
and
$$G_x = \{g \in G : gxg^{-1} = x\} = C(g).$$
That is, the orbit of x is the conjugacy class of x in G and the stablizer subgroup of x is the centralizer of x.

Claim: The collection of conjugacy classes of G partition G.

Proof. Notice that each $x \in G$ is in its own conjugacy class since $x = exe^{-1}$ where e is the identity element. Suppose now that $y \in a^G \cap b^G$. Then
$$gag^{-1} = y = hbh^{-1}$$
for some $g, h \in G$. Rearranging this equation implies that $a \in b^G$. From here, it follows that $a^G \subseteq b^G$ and similarly $b^G \subseteq a^G$. That is, conjugacy classes are either disjoint or equal.

Since the set of conjugacy classes of G partition G,
$$|G| = \sum_{x \in J} |x^G|$$
where J is a list consisting of one element from each conjugacy class of G. If a conjugacy class with representative z is of size one, then $gzg^{-1} = z$ for each $g \in G$. That is, $z \in Z(G)$. If $z \in Z(G)$, then $\{gzg^{-1} : g \in G\} = \{z\}$. Therefore, the number of trivial conjugacy classes is equal to $|Z(G)|$. Therefore, if I is the list of elements in J that are not in $Z(G)$,
$$|G| = |Z(G)| \sum_{x \in I} |x^G|.$$

From the previous result,

$$|G| = |Z(G)| + \sum_{x \in I} [G : G_x] = \sum_{x \in I} [G : C(x)].$$

□

Proof. Let $|G| = p^k$ for some prime p and some $k \in \mathbb{N}$. The class equation implies that

$$|G| = |Z(G)| + \sum_{x \in I} [G : C(x)]$$

for some indexing set I as defined previously. Each $[G : C(x)]$ is of size greater than one and must divide $|G|$. Therefore each $[G : C(x)]$ is some power of p. This means that p must divide $|Z(G)|$ and so $|Z(G)|$ is nontrivial. □

Problem 4.32: F12

Define the center of a group.

(a) Prove that if the order of G is p^k for some prime p then G has nontrivial center.

(b) Suppose that p and q are distinct primes. Prove that a non-abelian group of order pq has trivial center.

The center of a group G is the subgroup

$$Z(G) = \{g \in G : gx = xg \text{ for any } x \in G\}$$

Proof. Assume that $|G| = p^k$ for some prime p. If $k = 1$, then G is cyclic and therefore abelian. In this case, $Z(G) = G$ and thus is nontrivial. Assume now that $k > 1$. If G is abelian, $Z(G) = G$ and so G has nontrivial center. If G is non-abelian, $G - Z(G)$ is non-empty. Let $C_1, \ldots, C_n$ be the distinct conjugacy classes of elements in $G - Z(G)$. That is, for each $j \in \{1, \ldots, n\}$ let $x_j \in G - Z(G)$ such that $C_j = \{gx_jg^{-1} : g \in G\}$. Note that each $|C_j| > 1$ since a conjugacy class is a singleton if and only if the representative element is in $Z(G)$. The Orbit Stablizer Theorem implies that for each $j = 1, \ldots, n$,

$$|C_j| = [G : C_G(x_j)]$$

where $C_G(x_j) = \{g \in G : gx_jg^{-1} = x_j\}$ is the centralizer of x_j in G. In particular, each $|C_j|$ divides $|G| = p^k$. Since $|C_j| > 1$, p divides each $|C_j|$. The Class Equation states that

$$|Z(G)| = |G| - \sum_{j=1}^{n} [G : C_G(x_j)] = p^k - \sum_{j=1}^{n} |C_j|.$$

Because p divides p^k and p divides each $|C_j|$, p must also divide $|Z(G)|$. Thus $Z(G)$ is nontrivial. □

Proof. See 4.27. □

Note that 4.33 is Cauchy's Theorem and comes up for many Sylow-like problems. There's another version of the proof specifically for the case when $p = 2$ that does not involve group actions.

Problem 4.33: F18.G1

Let G be a finite group with order that is divisible by a prime p. Prove that G contains an element of order p.

Proof. Assume that G is a finite group such that a prime p divides $|G|$. Define a set $X \subseteq G^p$ as

$$X = \{(x_1, \ldots, x_p) \in G^p : x_1 \cdots x_p = e\}.$$

That is, X is the set of all p-tuples of elements in G where the product of the elements is the identity in G. Note that by choosing $x_1, \ldots, x_{p-1}$, x_p is determined as

$$x^p = (x_1 \cdots x_{p-1})^{-1}.$$

This means that $|X| = G^{p-1}$ and therefore p must divide $|X|$.

Next observe that if $x_1 \cdots x_p = e$, multiplying $x_1, \ldots, x_p$ in any order yields the identity. That is, if $(x_1, \ldots, x_p) \in X$, any permutation of this p-tuple is also in X. Therefore, we may let $\mathbb{Z}/p\mathbb{Z}$ act on X via permutation. That is,

$$1 \cdot (x_1, \ldots, x_p) \mapsto (x_p, x_1, \ldots, x_{p-1}).$$

Since the order of $\mathbb{Z}/p\mathbb{Z}$ is prime, every stabilizer subgroup is either of size 1 or of size p. By the Order Stabilizer Theorem, this means that the order of an orbit is either 1 or p. Furthermore, the orbits of this action form a partition of X. Elements of X that are in an orbit of size 1 must be of the form $(x, \ldots, x)$ where $x^p = e$. Since $(e, \ldots, e) \in X$ satisfies this condition, e is in an orbit of size 1. Because orbits are of size 1 or p and partition X, there exists some $x \neq e$ also in an orbit of size 1. If this were not the case, p would not divide X, a contradiction. This chosen x is of order p since $x^p = e$. □

4.7 Automorphisms

Problem 4.34: F13.G2, S03.G2

Prove that every finite group of order greater than two has a non-trivial automorphism.

Proof. Suppose first that G is a non-abelian group of order greater than two. Since G is non-abelian, there exists an element $g \in G \setminus Z(G)$. Then, the homomorphism $\varphi : G \to G$ given by $\varphi(x) = gxg^{-1}$ is non-trivial since there exists $x \in G$ where $gx \neq xg$. If $gxg^{-1} = gyg^{-1}$, then right and left multiplying by g and g^{-1}, respectively, yields that $x = y$. Therefore φ is a non-trivial automorphism.

Suppose now that G is abelian. If G is a 2-group, then $G \cong \mathbb{Z}_2^k$ for some $k \in \mathbb{N}$. Consider the automorphism $\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ given by

$$\varphi : (x_1, \ldots, x_k) \mapsto (x_2, x_1, \ldots, x_k).$$

Then φ is a nontrivial automorphism, by construction. Composing φ with the isomorphism between G and $\mathbb{Z}_2^k$ yields the desired automorphism of G.

If G is not a 2-group, then there exists some prime $p \neq 2$ that divides the order of G. By Cauchy's Theorem (see 4.33), there exists an element $x \in G$ of order p. The map $\varphi : g \mapsto g^{-1}$ is then a non-trivial automorphism as $\varphi(x) \neq x$. □

Problem 4.35: F18.G3, F03.G3

Let Inn(G) be the group of inner automorphisms of the group G and Aut(G) the group of all automorphisms of G.

(a) Show that Inn(G) is normal in Aut(G).

(b) Show that if $Z(G)$ is the center of G, then Inn(G) $\cong$ G/Z(G).

The 2003 version of this question only asks part (a), but also requires that we prove that Inn(G) *is a subgroup of* Aut(G)*.*

Proof. Let $\psi : G \to G$ be an automorphism. We must show that $\psi \text{Inn(G)} \psi^{-1} = \text{Inn(G)}$. Let $\varphi_g \in \text{Inn(G)}$ be the inner automorphism such that $\varphi_g : x \mapsto gxg^{-1}$. For any $x \in X$,

$$\psi\varphi_g\psi^{-1}(x) = \psi\left(g\psi^{-1}(x)g^{-1}\right) = \psi(g)x\psi(g)^{-1}$$

where the last equality follows from the fact that ψ is an automorphism. Therefore, $\psi\varphi_g\psi = \varphi_{\psi(g)} \in$ Inn(G). □

Proof. Define a map $F : G \to \text{Inn(G)}$ by $F : g \mapsto \varphi_g$ where $\varphi_g : x \mapsto gxg^{-1}$. For any $g, h \in G$ and $x \in G$,

$$\begin{aligned}\varphi_g \circ \varphi_h(x) &= \varphi_g\left(hxh^{-1}\right)\\ &= ghxh^{-1}g^{-1}\\ &= (gh)x(gh)^{-1}\\ &= \varphi_{gh}(x).\end{aligned}$$

Therefore, $F(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h = F(g)F(h)$. By construction, F is surjective. If $g \in Z(G)$, then $gxg^{-1} = xgg^{-1} = x$ for every $x \in G$. That is, φ_g is the identity element in Inn(G) and so $Z(G) \subseteq \ker(F)$. If φ_g is the identity map, then $gxg^{-1} = x$ for all $x \in G$. Equivalently, $g \in Z(G)$. Since $F(G) = \text{Inn(G)}$ and $\ker(F) = Z(G)$, the First Isomorphism Theorem implies that $\text{Inn(G)} \cong \text{G/Z(G)}$, as desired. □

5 Rings and Fields

5.1 General Rings and Fields

Problem 5.1: (S03.RF1)

Let $V = \mathbb{R}^2$, regarded as a 2-dimensional vector space over $\mathbb{R}$. Let $L(V)$ denote the ring of all linear transformations from V to V. Let $T \in L(V)$ be defined by $T(x, y) = (y, -x)$ and define

$$A = \{S \in L(V) : ST = TS\}.$$

(a) Prove that A is a subring of $L(V)$.

(b) To which well-known ring is A isomorphic? Give the isomorphism.

Proof. Let $I \in L(V)$ denote the identity transformation. Because $IT = TI$, it follows that $I \in A$. Suppose now that $R, S \in A$ and consider the linear transformation $R - S \in L(V)$. Then,

$$(R - S)T = RT - ST = TR - TS = T(R - S)$$

implying that $R - S \in A$. Similarly,

$$(RS)T = R(ST) = R(TS) = (RT)S = (TR)S = T(RS)$$

proving that $RS \in A$. As A is nonempty, closed under addition, additive inverses, and multiplication, A is a subring. □

Claim: $A \cong \mathbb{C}$.

Proof. With respect to the standard basis for $\mathbb{R}^2$, the matrix of T is

$$M(T) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Given any $a, b \in \mathbb{R}$, define $S_{a,b} \in L(V)$ by $S_{a,b}(x, y) = (ax + by, -bx + ay)$. Note that $S_{a,b} \in A$ since

$$ST(x, y) = S(y, -x) = (ay - bx, -by - ax) = T(ax + by, ay - bx) = TS(x, y)$$

for each $(x, y) \in V$. Now define $\varphi : \mathbb{C} \to A$ by

$$\varphi(a + bi) = S_{a,b}.$$

If $\varphi(a + bi) = \varphi(c + di)$, then $S_{a,b}(x, y) = S_{c,d}(x, y)$ for each $(x, y) \in V$. In particular,

$$(a, -b) = S_{a,b}(1, 0) = S_{c,d}(1, 0) = (c, -d)$$

implying that $a + bi = c + di$ and thus φ is injective. To see that φ is surjective, consider any $S \in A$. If the matrix of S with respect to the standard basis is $M(S) = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$, then

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & v \\ w & z \end{pmatrix} = \begin{pmatrix} u & v \\ w & z \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Equivalently,

$$\begin{pmatrix} v & -u \\ z & -w \end{pmatrix} = \begin{pmatrix} -w & -z \\ u & v \end{pmatrix}.$$

Therefore,

$$M(S) = \begin{pmatrix} u & v \\ w & z \end{pmatrix} = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$$

meaning that $S = S_{u,v}$. That is, $\varphi(u + vi) = S_{u,v} = S$.

The computations to verify that φ is a homomorphism are straightforward and standard.

Problem 5.2: (F17.RF3, S03.RF3)

Let p be a prime and $\mathbb{F}_p$ the field of p elements. Let x be an indeterminate and let $R_1 = \mathbb{F}_p[x]/(x^2-2)$ and $\mathbb{R}_2 = \mathbb{F}_p[x]/(x^2-3)$. Determine whether or not the rings R_1 and R_2 are isomorphic when

(a) $p = 5$

(b) $p = 11$

Solution. When $p = 5$, neither $x^2 - 2$ nor $x^2 - 3$ has any roots in $\mathbb{F}_5$. Therefore both of these polynomials are irreducible. By Kronecker's Theorem, R_1 and R_2 are both fields of order $5^2 = 25$. Since there is only one field of order 25, $R_1 \cong R_2$.

Now let $p = 11$. In this case, 5 is a root of $x^2 - 3$. Therefore, R_2 is not a field. However, $x^2 - 2$ is irreducible in $\mathbb{F}_{11}$ since it has no roots. Therefore, R_1 is a field and $R_1 \ncong R_2$.

Problem 5.3: (S20.RF2), (F14.G2)

Let K be a field. Show that every finite subgroup of $K^\times$ is cyclic.

Proof. Let $G \leq K^\times$ be a finite subgroup. Then G is a finite abelian group and can therefore can be written as the direct product of its Sylow subgroups, each of some prime power order. By the Chinese Remainder Theorem, this direct product is cyclic if and only if each of the Sylow subgroups is cyclic. Therefore, without loss of generality, assume that $|G| = p^k$.

Let m denote the maximal order of the elements in G. That is, $m \leq p^k$ and $g^m - 1 = 0$ for each $g \in G$. This means that each $g \in G$ is a root of $x^m - 1$. Since G is a field, this polynomial has at most m roots. Therefore $m = p^k$ and so G has an element of order m which generates the subgroup. □

Problem 5.4: F16.RF3

Let p be a prime and R_p the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbb{Z}_p$.

(i) Show that R_p is a commutative ring with identity.

(ii) Show that R_7 is a field.

(iii) Show that R_{13} is not a field.

Proof. Let $S, T \in R_p$ be arbitrary. Both ST and $S + T$ are in R_p, by properties of modular arithmetic. Notice that $ST = TS$, following from the definition of matrix multiplication and the commutativity of $\mathbb{Z}_p$. Similarly, $S + T = T + S$. The additive inverse of S is $-S$ which is in R_p. The multiplicative identity in R_p is the 2×2 identity matrix and the additive identity is the 2×2 zero matrix. □

Proof. From (i), R_7 is a commutative ring with identity. It remains to show that each element of R_7 has a multiplicative inverse. Let $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in R_7$ be nonzero. Then at most one of a and b can be zero. Consider the quantity $a^2 + b^2 \in R_7$. In R_7, $a^2, b^2 \in \{0, 1, 2, 4\}$. At most one of a^2 and b^2 can be zero and upon inspection this implies $a^2 + b^2 \neq 0$. Therefore, $a^2 + b^2$ has an inverse in R_7. The matrix

$$\begin{pmatrix} a\left(a^2+b^2\right)^{-1} & -b\left(a^2+b^2\right)^{-1} \\ b\left(a^2+b^2\right)^{-1} & a\left(a^2+b^2\right)^{-1} \end{pmatrix}$$

is therefore well-defined and is the multiplicative inverse of the original matrix. □

Solution. Consider the matrix $\begin{pmatrix} 2 & 3 \\ -3 & 2 \end{pmatrix} \in R_{13}$. Because $2^2+3^2 = 0$ in $\mathbb{R}_{13}$, there is no multiplicative inverse for the matrix.

5.2 Ideals

Problem 5.5: S18.RF1

Let R be a commutative ring with 1 and let M be an ideal of R. Prove that when M is both maximal and principal there are no ideals properly between M^2 and M.

Proof. Since M is a principal ideal, there exists $a \in R$ such that $M = (a)$. Then, $M^2 = (a^2)$. Suppose that J is an ideal of R such that $M^2 \subseteq J \subseteq J$. Furthermore, assume that $J \neq M$. We shall prove that this implies $J = M^2$.

Since $J \neq M$, there exists $x \in M \setminus J$. Then, $x = ra$ for some $r \in R$. If $rM = M$ then $r = r'a$ for some $r' \in R$. This means that $x = ra = (r'a)a = r'a^2 \in M^2$. But $x \notin J$ so $x \notin M^2$. Therefore, $rM \neq M$ and so the ideal $rM + M$ contains M as a proper subideal. Because M is maximal and $M \subset rM + M \subseteq R$, it must be the case that $rM + M = R$. In particular, there exist $s, t \in R$ such that

$$1 = rsa + ta.$$

Multiplying both sides of the equation by a implies that

$$a = rsa^2 + ta^2 \in M^2$$

and as a generates M, it follows that $M \subseteq M^2$. Therefore, $J \subseteq M = M^2$ and so $J = M^2$. □

Problem 5.6: F19.RF1

Prove that the set N of nilpotent elements of a commutative ring R is an ideal of R and that R/N has no nilpotent elements.

Proof. Since $0^1 = 0$, $0 \in N$ and thus $N \neq \varnothing$. Suppose that $x, y \in N$ are nonzero with $x^n = y^m = 0$ for some $m, n > 1$. Since R is commutative,

$$(x+y)^{mn} = \sum_{k=0}^{mn} \binom{mn}{k} x^k y^{mn-k}$$

via the Binomial Theorem. Without loss of generality, assume that $n \leq m$. Then whenever $m \leq k \leq mn$, $x^k = 0$. Whenever $0 \leq k \leq m$, $m(n-1) \leq mn - k \leq mn$. This implies that $k \geq m(n-1) \geq n(n-1) \geq n$ and therefore $y^k = 0$. Therefore $(x+y)^{mn} = 0$ and so $x + y \in N$. For any $r \in R$, $(rx)^n = r^n x^n = r^n \cdot 0 = 0$ where the first equality follows from R being commutative. Therefore $rx \in N$. As N is closed under addition and multiplication by elements in R, N is an ideal.

Suppose that R/N has some nonzero nilpotent element. That is there exists $r \in R - N$ and $m \geq 1$ such that $(r+N)^m = N$. This implies that $r^m \in N$. Choose $n \geq 1$ such that $(r^m)^n = 0$. But this means that $r^{mn} = 0$, contradicting that $r \notin N$. Thus there are no nonzero nilpotent elements in R/N. □

Problem 5.7: S11.RF2

Let R be a commutative ring with 1. Show that an ideal M is maximal if and only if for all $r \in R \setminus M$ there exists an element $x \in R$ such that $1 - rx \in M$.

Proof. Suppose first that M is a maximal ideal. Then R/M is a field. Let $r \in R \setminus M$ so that $r + M \in R/M$ is a nonzero element. As R/M is a field, there exists $x + M \in R/M$ such that $(r+M)(x+M) = 1 + M$. By the definitions of multiplication and addition in R/M, $1 - rx + M = M$ implying that $1 - rx \in M$.

Let $r+M \in R/M$ be a nonzero element. Then $r \in R \setminus M$ and so there exists $x \in \mathbb{R}$ such that $1-rx \in M$. This means that $M = (1-rx)+M = (1+M)-(r+M)(x+M)$. Rearranging, we see that $(r+M)(x+M) = 1+M$ meaning that $r + M$ has a multiplicative inverse in R/M. As $r + M$ was an arbitrary nonzero element, it follows that R/M is a field and so M must be a maximal ideal. □

5.3 Nilpotent

Problem 5.8: S19

Prove the following:

(a) If R is a commutative ring with no nilpotent elements, then $R[x]$ has no nilpotent elements.

(b) If r is a nilpotent element of a ring with unity, then $1 - r$ is a unit.

Proof. Suppose that $a_0 + a_1x + \cdots + a_nx^n = p(x) \in R[x]$ is nilpotent. Then there exists $k \in \mathbb{N}$ such that $p(x)^k = (a_0 + a_1x + \cdots + a_nx^n)^k = 0$. In particular, the leading coefficient of $p(x)^k$ is a_n^k and since $p(x)^k = 0$, $a_n^k = 0$. Since a_n is the leading term of $p(x)$, it is nonzero and therefore a nilpotent element of R. □

Proof. Suppose that r is nilpotent. Choose a minimal $k \in \mathbb{N}$ such that $r^k = 0$. Then,

$$1 = 1 - r^k = (1 - r)(1 + r + r^2 + \cdots + r^{k-1})$$

meaning that $1 - r$ has multiplicative inverse given by $(1 + r + r^2 + \cdots + r^{k-1})$. That is, $1 - r$ is a unit. □

Problem 5.9: F14.RF3

Prove that the set N of nilpotent elements of a commutative ring R is an ideal of R and that R/N has no nonzero nilpotent elements.

Proof. Suppose that $x, y \in N$. Let $m, n \in \mathbb{N}$ be such that $x^m = 0$ and $y^n = 0$. Then,

$$(xy)^m = x^m y^m = 0$$

meaning that $xy \in N$. Since R is commutative, the Binomial Expansion Theorem holds and so

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}.$$

Observe that whenever $k \geq m$, $x^k = 0$ and whenever $k \geq n$, $y^k = 0$. When $0 \leq k \leq m$, $m + n - k \geq n$ and therefore, $\binom{m+n}{k} x^k y^{m+n-k} = 0$. When $m \leq k \leq m + n$, $\binom{m+n}{k} x^k y^{m+n-k} = 0$. Therefore, $(x + y)^{m+n} = 0$ meaning that $x + y \in N$.

Assume now that $r \in R$ is arbitrary. Then,

$$(rx)^m = r^m x^m = 0$$

and so $rx \in N$. As R is a commutative ring, this proves that N is an ideal of R. □

Proof. Suppose that $r + N$ is nilpotent in R/N. Choose $m \in \mathbb{N}$ such that $(r + N)^m = N$. For this m, it follows that $r^m + N = N$ or equivalently, $r^m \in N$. Since $r^m \in N$, there exists $n \in \mathbb{N}$ where $(r^m)^n = 0$. But this means that $r^{mn} = 0$ and so $r \in N$. Thus, any nilpotent element of R/N is zero. □

Problem 5.10: (F12.RF3)

(a) Prove that $\mathbb{Z}/m\mathbb{Z}$ has no non-zero nilpotent elements if and only if m has no multiple prime factor.

(b) Prove that every element of $\mathbb{Z}/m\mathbb{Z}$ is either nilpotent or a unit whenever m is a prime power.

(c) Prove that if r is a nilpotent element of a ring with unity then $1 - r$ is a unit.

Proof. Suppose first that m has some multiple prime factor. If $p_1, \ldots, p_n$ are the distinct prime factors of m, this implies that there exists $k \geq 2$ for which some $p_j^k | m$. In particular, this means that the product $p_1 \cdots p_n$ is not congruent to zero modulo m. Write out the prime factorization for m as

$$m = p_1^{\ell_1} \cdots p_n^{\ell_n}$$

and define $d = \gcd \ell_1, \ldots, \ell_n$. Then, $(p_1 \cdots p_n)^d = 0$ in $\mathbb{Z}/m\mathbb{Z}$ and thus is a nonzero nilpotent element.

Now suppose that $m = p_1 \cdots p_n$ with $p_1, \ldots, p_n$ the distinct prime factors of m. That is, m has no multiple prime factors. Let $x \in \mathbb{Z}/m\mathbb{Z}$ be such that $x^k = 0$ for some $k \in \mathbb{N}$. Write $x = q_1^{\ell_1} \cdots q_r^{\ell_r}$ where each q_j is prime, the q_j are distinct, and $0 \leq x < m$. Then, $x^k = q_1^{k\ell_1} \cdots q_r^{k\ell_r}$. Since m divides x^k, each p_j must divide x^k. Since the q_i and p_j are all prime, this means that $p_j = q_i$ for some i. But, x and x^k share the same prime factors and so each p_j must divide x. Therefore, m divides x and so $x = 0$ in $\mathbb{Z}/m\mathbb{Z}$. It follows that any nilpotent element in such a $\mathbb{Z}/m\mathbb{Z}$ must be zero. □

Proof. Let p be prime and suppose that $m = p^N$ for some $N \in \mathbb{N}$. Let $x \in \mathbb{Z}/m\mathbb{Z}$ and suppose first that p divides x. Then $x = pq$ for some q. Observe that

$$x^N = (pq)^N = p^N q^N = 0$$

since $p^N = m \equiv 0$ in $\mathbb{Z}/m\mathbb{Z}$. That is, whenever p divides x, it follows that x is nilpotent. Suppose now that p does not divide x. Because the only divisors of m are powers of p, the greatest common divisor of m and x is 1. Therefore there exist integers s, t where $1 = xs + mt$. As $mt = 0$ in $\mathbb{Z}/m\mathbb{Z}$, $xs = 1$ implying that x is a unit. □

Proof. Assume that $r \in R$ is a nilpotent element of a ring with unity. Then there exists $n \in \mathbb{N}$ such that $r^n = 0$. Then,

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

meaning that $\sum_{i=0}^{n-1} r^i$ is the multiplicative inverse of $(1 - r)$. That is, $1 - r$ is a unit. □

5.4 Polynomial Rings

Problem 5.11: (S20.RF4)

Prove that the polynomial $x^3 - 2$ is irreducible over the field $\mathbb{Q}(i)$.

Proof. Let $f = x^3 - 2$. Notice that f is irreducible over $\mathbb{Q}$ by Eisenstein's Theorem. If ζ denotes a primitive 3rd root of unity, then the three roots of f are $a, a\zeta, a\zeta^2$. That is, $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a\zeta) : \mathbb{Q}] = [\mathbb{Q}(a\zeta^2) : \mathbb{Q}] = 3$

If f were to be reducible over $\mathbb{Q}(i)$, then f would have a root in $\mathbb{Q}(i)$. Seeking a contradiction, let $\alpha \in \mathbb{Q}(i)$ be a root of f. Then, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i)$ is a subfield. Since $x^2 + 1$ is irreducible over $\mathbb{Q}$ and has i as a root, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. By Tower Rule, $2 = [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. But, a is a root of f and therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, a contradiction. □

Problem 5.12: (F20.RF1)

The polynomial $x^3 - x$ has six roots in the ring $\mathbb{Z}/6\mathbb{Z}$. Find a sufficient condition on a commutative ring R which ensures that the number of roots of a polynomial with coefficients in R cannot exceed its degree and justify your assertion.

Claim: If R is a field and $f \in R[x]$ is a nonzero polynomial of degree n, then f has at most n roots in R.

Proof. We proceed by induction on the degree of f. If $\deg(f) = 0$, then f is constant and nonzero, meaning it has no zeros. Assume that $\deg(f) = 1$ so that $f(x) = ax + b$ for some $a, b \in R$. If r, s are both roots of f, then

$$ar + b = as + b$$

and therefore $r = s$. That is, f has at most one root in R.

Now let $\deg(f) = n$ and assume that the result holds for any polynomial p of degree less than n. If f has no zeros in R, then the result holds. Otherwise, suppose that r is a root of f in R. Then, $f(x) = (x - r)q(x)$ where $q \in R[x]$ is a polynomial of degree $n - 1$. By the inductive hypothesis, q has at most $n - 1$ roots and therefore f has at most n roots.

5.5 Finite Fields

Problem 5.13: (F03.RF1)

Give an explicit construction for a field F of 9 elements.

Proof. Let $K = \mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$ be the field of 3 elements. Consider the polynomial $f(x) = x^2+1 \in K[x]$. Since f is a degree-two polynomial, f is reducible if and only if f has a root in K. But, $f(0) = 1, f(1) = 2, f(-1) = 2$. Thus, f is irreducible in $K[x]$ and by Kronecker's Theorem, $F = K[x]/(x^2 + 1)$ is a field of $3^2 = 9$ elements. The elements of F are

$$\begin{array}{ccc} 0 + (x^2+1) & 1 + (x^2+1) & 2 + (x^2+1) \\ x + (x^2+1) & x + 1 + (x^2+1) & x + 2 + (x^2+1) \\ 2x + (x^2+1) & 2x + 1 + (x^2+1) & 2x + 2 + (x^2+1) \end{array}$$

□

Problem 5.14: (S04.RF1)

Let F be a finite field. Using only vector space theory, prove that if $|F| = p^m$ and K is an extension field of F with $|K| = p^n$, then m divides n.

Proof. Note first that both F and K contain a copy of $\mathbb{F}_p$.

Claim: Let F be a finite field of characteristic p. Then, $|F| = p^n$ if and only if $[F : \mathbb{F}_p] = n$.

Proof. Since char(F) = p, there exists a subfield L of F that is isomorphic to $\mathbb{F}_p$. Therefore, F can be viewed as an $\mathbb{F}_p$-vector space. Let $\{x_1, \ldots, x_n\}$ be an $\mathbb{F}_p$-basis for F. A basic counting argument and the definition of the degree of an extension then implies that $[F : \mathbb{F}_p] = n$ if and only if $|F| = p^n$.

From the claim, $[F : \mathbb{F}_p] = m$ and $[K : \mathbb{F}_p] = n$. As F is a subfield of K, there exists an F-basis, say $\{k_1, \ldots, k_r\}$ for K. That is, for each $k \in K$ there exist unique $b_1, \ldots b_r \in F$ such that

$$k = b_1 k_1 + \cdots b_r k_r.$$

Similarly, there exists an $\mathbb{F}_p$-basis, say $\{f_1, \ldots, f_m\}$, for F. Then each b_i can be written uniquely in the form

$$b_i = a_1 f_1 + \cdots + a_m f_m$$

with each $a_1, \ldots, a_m \in \mathbb{F}_p$. A counting argument can then be used to see that $p^n = |K| = (p^m)^r$. That is, $p^n = p^m r$ and therefore m divides n, as desired. □

Problem 5.15: (S04.RF1.ab, F18.RF1)

(a) Define the characteristic of a field. Prove that a finite field must have prime characteristic p and deduce that it has p^k elements for some $k \in \mathbb{N}$.

(b) Prove that a finite field cannot be algebraically closed.

(c) Construct a field of 125 elements.

Proof. Let F be a finite field. Since F is finite, the cyclic additive group generated by 1 is finite. Therefore, the characteristic of F is finite.

Seeking a contradiction, suppose that the characteristic of F is some composite number $m \cdot n$. Then,

$$0 = (mn) \cdot 1 = m \cdot (1 + \cdots + 1) = (1 + \cdots + 1)_{m \text{ times}}(1 + \cdots + 1)_{n \text{ times}}.$$

But this is a contradiction since F cannot have any zero divisors and mn is defined to be minimal. Therefore the characteristic of F is prime.

Let p be the prime characteristic of F. Then the prime field of F is isomorphic to $\mathbb{F}_p$. This means that $[F : \mathbb{F}_p] = k$ for some $k \in \mathbb{N}$. Viewing F as a vector space over $\mathbb{F}_p$, it follows that F has p^k elements. □

Proof. Let F be a finite field of order p^k. Enumerate the elements of f as $\alpha_1, \ldots, \alpha_{p^k}$. Consider the polynomial in $F[x]$ given by

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_{p^k}) + 1.$$

Then $f(\alpha_j) = 1$ for each $j = 1, \ldots, p^k$. Since f is a polynomial over F with no roots in F, F is not algebraically closed. □

Solution. Let $\mathbb{F}_5$ be the finite field with 5 elements and consider the polynomial $f(x) = x^3 + x^2 + x + 3$. If f is reducible, then f must have a root in $\mathbb{F}_5$. However, $f(0) = 3, f(1) = 1, f(2) = 2, f(3) = 2$, and $f(4) = 2$. Therefore f is irreducible. By Kronecker's Theorem,

$$F = \mathbb{F}_5/(f)$$

is a field and has 5^3 elements.

Problem 5.16: (S20.RF2)

Let $\mathbb{F}_3$ be the field with 3 elements.

(a) Prove that $K = \mathbb{F}_3[x]/(x^2+1)$ is a field.

(b) How many elements does K have?

(c) Prove that $x+1$ generates the multiplicative group of non-zero elements in K.

Proof. Let $f = x^2+1$. The only way for f to be reducible over $\mathbb{F}_3$ is if f has a root in $\mathbb{F}_3$. However this is impossible since $f(0) = 1$, $f(1) = 2$, and $f(2) = 2$. By Kronecker's Theorem, a polynomial ring quotiented out by an ideal generated by an irreducible polynomial is a field. □

Solution. Let $\overline{1}$ and $\overline{x}$ denote the images of $1, x \in \mathbb{F}_3[x]$ under the quotient map. By Kronecker's Theorem, $\{\overline{1}, \overline{x}\}$ form a basis for $\mathbb{F}_3[x]/(x^2+1)$ over $\mathbb{F}_3$. Therefore there are $3^2 = 9$ elements in K.

Proof. Since $|K| = 9$, the multiplicative group will have eight elements. Let $I = (x^2+1)$. Through algebraic manipulations, we see that

$$\begin{aligned}(x+1+I)^2 &= 2x+I\\ (x+1+I)^3 &= 1+2x+I\\ (x+1+I)^4 &= 2+I\\ (x+1+I)^5 &= 2+2x+I\\ (x+1+I)^6 &= x+I\\ (x+1+I)^7 &= 2+x+I\\ (x+1+I)^8 &= 1+I\end{aligned}$$

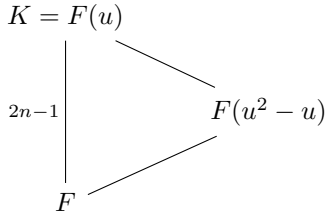
proving that $1+x+I$ generates K^*. □

5.6 Field Extensions

Problem 5.17: (F04.RF1)

Suppose that $K = F(u)$ is a finite field extension of F such that the degree $[K : F]$ is odd. Show that $K = F(u^2-u)$.

Proof. Since $F(u)$ is a field containing u, $u^2 - u \in F(u)$. Thus, $F(u^2-u) \subseteq F(u)$ and we may consider the following diagram:



for some $n \in \mathbb{N}$. Seeking a contradiction, suppose that $[F(u) : F(u^2-u)] > 1$. In particular, this means that $u \notin F(u^2-u)$. The minimal polynomial for u over $F(u^2-u)$ is

$$f(x) = x^2 - x - (u^2-u)$$

since the degree of the minimal polynomial is at least degree two and f has u as a root. Therefore, $[F(u) : F(u^2-u)] = 2$. By the Tower Rule, this means that 2 must divide $[K : F]$, contradicting the assumption that the degree was odd. Therefore, $[F(u) : F(u^2-u)] = 1$, or equivalently, $F(u) = F(u^2-u)$ as desired. □

Problem 5.18: (F03.RF2)

Suppose that $\alpha \neq 0$ is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd. Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha + \alpha^{-1})$. Must this be true without the assumption that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd?

Proof. Since $\mathbb{Q}(\alpha)$ is a field containing α, it also must contain $\alpha + \alpha^{-1}$ and so $\mathbb{Q}(\alpha + \alpha^{-1}) \subseteq \mathbb{Q}(\alpha)$. Tower Rule implies that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha + \alpha^{-1}) :] \cdot [\mathbb{Q}(\alpha + \alpha^{-1}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Notice that α is a root of the polynomial $x^2 - (\alpha + \alpha^{-1})x + 1 \in \mathbb{Q}(\alpha + \alpha^{-1})[x]$. Therefore, $[\mathbb{Q}(\alpha + \alpha^{-1}) : \mathbb{Q}]$ is either 1 or 2. But $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd and therefore $[\mathbb{Q}(\alpha + \alpha^{-1}) : \mathbb{Q}] = 1$. This implies that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha + \alpha^{-1})$, as desired. □

If the assumption that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd is removed, this statement is false. Consider the extension $\mathbb{Q}(i)$ over $\mathbb{Q}$. This is a degree 2 extension, but $\mathbb{Q}(i + i^{-1}) = \mathbb{Q}(i + (-i)) = \mathbb{Q} \neq \mathbb{Q}(i)$.

Problem 5.19: (F17.RF2, S03.RF2)

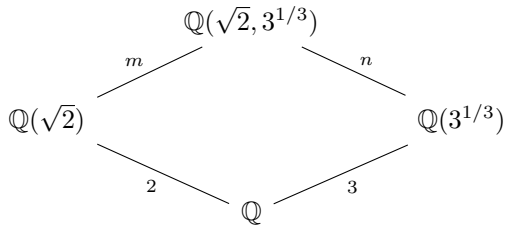
(i) State Eisenstein's irreducibility criterion for polynomials.

(ii) Find $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ and $[\mathbb{Q}(3^{1/3}) : \mathbb{Q}]$.

(iii) Using (ii), prove that $\alpha = \sqrt{2} + 3^{1/3}$ is irrational.

Proof. The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ and therefore $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Similarly, the minimal polynomial for $3^{1/3}$ over $\mathbb{Q}$ is $x^3 - 3$ and so $[\mathbb{Q}(3^{1/3}) : \mathbb{Q}] = 3$. □

Proof. Seeking a contradiction, suppose that $\alpha \in \mathbb{Q}$.



Because $\alpha \in \mathbb{Q}$, $3^{1/3} = \alpha - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Therefore, $[\mathbb{Q}(\sqrt{2} + 3^{1/3}) : \mathbb{Q}(\sqrt{2})] = m = 1$. Similarly, $\sqrt{2} = \alpha - 3^{1/3} \in \mathbb{Q}(3^{1/3})$ and so $[\mathbb{Q}(\sqrt{2} + 3^{1/3}) : \mathbb{Q}(3^{1/3})] = n = 1$. However, the Tower Rule implies that $2 = m \cdot 2 = n \cdot 3 = 3$, a contradiction. □

5.7 Galois Groups

Problem 5.20: (F14.RF2)

(a) Find a monic polynomial $f(x) \in \mathbb{Q}[x]$ that has $\sqrt{1 + \sqrt{2}}$ as a root.

(b) Find the splitting field K of $f(x)$ over $\mathbb{Q}$.

(c) Find the Galois group of K over $\mathbb{Q}$.

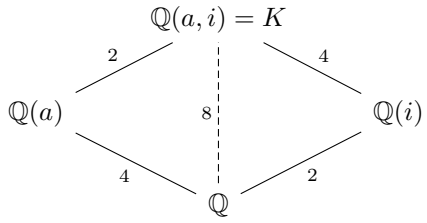
Solution. Consider the polynomial $x^4 - 2x^2 - 1$. Upon inspection, this polynomial has $\sqrt{1 + \sqrt{2}}$ as a root and is monic.

Solution. Let $f(x) = x^4 - 2x^2 - 1$. The roots of f are

$$\sqrt{1+\sqrt{2}}$$
$$\sqrt{1-\sqrt{2}}$$
$$-\sqrt{1+\sqrt{2}}$$
$$-\sqrt{1-\sqrt{2}}$$

Notice that since $1 - \sqrt{2} < 0$, the splitting field for f must contain complex values. Let $a = \sqrt{1+\sqrt{2}}$ and $b = \sqrt{1-\sqrt{2}}$. Define $c = \sqrt{\sqrt{2}-1}$ so that $b = ic$. Upon inspection, $a^{-1} = c$. Define $K = \mathbb{Q}(a, i)$. Then K contains $\pm a$, by additive closure. Since $a^{-1} = c$, $ia^{-1} = ic = b$ must also be in K. Therefore K contains all four roots of f and thus is a splitting field.

Solution. Consider the following diagram:



From (a), we know that a is a root of an irreducible degree 4 polynomial and so $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Since both $\mathbb{Q}$ and $\mathbb{Q}(a)$ are real-valued fields, $[\mathbb{Q}(a, i) : \mathbb{Q}(a)] = 2$ and $[Q(i) : \mathbb{Q}] = 2$. The remaining degrees in the diagram follow directly from Tower Rule.

Solution. From (b), it follows that $|G(K : \mathbb{Q})| = 8$ since the order of the Galois group equals the degree of the splitting field over the base field.

Let $f = x^4 - 2x^2 - 1$. Then f is irreducible over $\mathbb{Q}$ and has a as a root. For simplicity, let $a_1 = a, a_2 = -a, a_3 = b, a_4 = -b$ denote the roots of f. By the Extension Lemma the identity map on $\mathbb{Q}$ can be extended to $\varphi_j : \mathbb{Q}(a) \to \mathbb{Q}(a_j)$ where $\varphi_j : a \mapsto a_j$. Apply the Extension Lemma again to each φ_j to obtain $\varphi_{j1} : \mathbb{Q}(a, i) \to \mathbb{Q}(a_j, i)$ where $\varphi_{j1} : i \mapsto i$ and $\varphi_{j2} : \mathbb{Q}(a, i) \to \mathbb{Q}(a_j, i)$ where $\varphi_{j2} : i \mapsto -i$. Here, $\pm i$ are the roots of the irreducible polynomial $x^2 + 1$ over $\mathbb{Q}(a)$. Upon inspection, $K = \mathbb{Q}(a, i) = \mathbb{Q}(a_j, i)$ and therefore each of the eight φjk is a $\mathbb{Q}$-automorphism. Since $|G(K : \mathbb{Q})| = 8$, these are all of the automorphisms.

The automorphism that sends a to b and i to i is of order four. Furthermore, the Galois group is nonabelian since the automorphism of order four does not commute with the automorphism that sends a to itself and i to $-i$. Therefore $G(K : \mathbb{Q}) \cong D_8$.

Problem 5.21: (S11.RF3), (S18.RF3)

Let F be a splitting field of the polynomial $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. Find the degree $[F : \mathbb{Q}]$ and determine the Galois group of the extension $\mathbb{Q} \subseteq F$ up to isomorphism.

Proof. Let $a = \sqrt[4]{2}$ and observe that $\{a, ai, -a, -ai\}$ are all roots of f. Since $\deg(f) = 4$, these are the only roots of f. By Eisenstein's Criterion, f is irreducible over $\mathbb{Q}$. Therefore f is the minimal polynomial for a over $\mathbb{Q}$ and so $[\mathbb{Q}(a), \mathbb{Q}] = 4$. Since $\mathbb{Q}(a)$ is a real-valued field, $i \notin \mathbb{Q}(a)$ and so the degree of the minimal polynomial for i over $\mathbb{Q}(a)$ is at least 2. But, i is a root of $x^2 + 1 \in \mathbb{Q}(a)[x]$ and so $[\mathbb{Q}(a, i) : \mathbb{Q}(a)] = 2$. By the Tower Rule, $[\mathbb{Q}(a, i) : \mathbb{Q}] = 4$. Since $\mathbb{Q}(a, i)$ contains all the roots of f, it is a splitting field for f over $\mathbb{Q}$

and thus is isomorphic to F. So, $[F : \mathbb{Q}] = 4$ as well.

Since $f(a) = 0$ and f is irreducible over $\mathbb{Q}$ The Extension Lemma yields isomorphisms $\varphi_k : \mathbb{Q}(a) \to \mathbb{Q}(ai^k)$ where $\varphi : a \mapsto ai^k$ for $k = 0, 1, 2, 3$. Next define $g(x) = x^2 + 1 \in \mathbb{Q}(a)$ and note that $g(i) = 0$ and g is irreducible over $\mathbb{Q}(a)$ as the roots are both complex. Again, by the Extension Lemma each φ_k may be extended to $\varphi_{k1} : \mathbb{Q}(a, i) \to \mathbb{Q}(ai^k, i)$ or $\varphi_{k2} : \mathbb{Q}(a, i) \to \mathbb{Q}(ai^k, -i)$ where

$$\varphi_{k1} : \begin{cases} a \mapsto ai^k \\ i \mapsto i \end{cases}$$

and

$$\varphi_{k2} : \begin{cases} a \mapsto ai^k \\ i \mapsto -i \end{cases}$$

Observe that this accounts for 8 $\mathbb{Q}$-automorphisms of $\mathbb{Q}(a, i)$. Since f has 4 roots and g has 2 roots and $\mathbb{Q}$-automorphisms must permute roots of polynomials over $\mathbb{Q}$, there are at most 8 total $\mathbb{Q}$-automorphisms. Thus $|G(\mathbb{Q}(a, i) : \mathbb{Q})| = 8$. Upon inspection, $G = G(\mathbb{Q}(a, i) : \mathbb{Q})$ is nonabelian and contains an element of order 4, φ_{11}. That is, $G \cong D_8$. □

6 Linear Algebra

6.1 Linear Maps

Problem 6.1: (S19.LA1)

Let V be a finite-dimensional vector space over a field F and $T : V \to V$ a linear map.

(a) If $F = \mathbb{C}$, prove that T has an eigenvalue.

(b) If $F = \mathbb{R}$, show that T need not have an eigenvalue.

Proof. See 3.2. □

Solution. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ have matrix representation given by

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

The characteristic polynomial of T is $x^2 + 1$ which has no real roots. Therefore T has no eigenvalues.

Problem 6.2: (F17.LA2, F13.LA1)

Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be a linear transformation. Prove the following:

(a) T has a one-dimensional invariant subspace.

(b) T has a two-dimensional invariant subspace.

Do not use the existence of canonical forms for matrices.

Proof. Let $p(x)$ be the characteristic polynomial of T. Since $T : \mathbb{R}^3 \to \mathbb{R}^3$, it follows that $\deg(p) = 3$. Therefore p has some real root, say λ. Then there exists a degree 2 polynomial $q(x) = x^2 + ax + b$ such that $p(x) = (x - \lambda)q(x)$.

Any real root of p corresponds to an eigenvalue of T. Therefore λ is an eigenvalue of T with some associated eigenvector, say v. The subspace span{v} is clearly a one-dimensional T invariant subspace.

Let $m(x)$ be the minimal polynomial of T. Then $m(x) = (x - \lambda)f(x)$ for some polynomial f of degree at most 2. By definition, m is the polynomial of smallest degree so that $m(T) = 0$. Define $K = \ker(f(T))$. If $\dim(K) = 3$, then $K = \mathbb{R}^3$ and $f(T) = 0$. This contradicts the minimality of m and therefore either $\dim(K) = 1$ or $\dim(K) = 2$.

If $\dim(K) = 1$, the rank-nullity theorem implies that $\text{range}(f(T)) = 2$. For any $v \in \mathbb{R}^3$,

$$(T - \lambda I)f(T)v = 0$$

since $m(T) = 0$. Therefore each element in $\text{range}(f(T))$ is an eigenvector associated with the eigenvalue λ. This means that $\text{range}(f(T))$ is a two-dimensional T-invariant subspace.

Now assume that $\dim(K) = 2$. For any $v \in K$, $f(T)v = 0$. Then,

$$f(T)(Tv) = T(f(T)v) = T(0) = 0$$

implying that $Tv \in \ker(f(T)) = K$. That is, K is a two-dimensional T-invariant subspace. □

Problem 6.3: (S18.LA3)

Let $T : V \to W$ be a linear transformation between two finite dimensional vector spaces. Prove that there exist bases for V and W such that the matrix representation for T with respect to these bases has an identity matrix in the top left corner and all other entries equal to zero.

Proof. Let $T : V \to W$ be a linear map. Let $v_1, \dots, v_n$ be a basis for (T). Extend this list to a basis $v_1, \dots, v_n, u_1, \dots, u_m$ for V.

Claim: The list $Tu_1, \dots, Tu_m$ is a basis for range(T).

Proof. Since $v_1, \dots, v_n, u_1, \dots, u_m$ form a basis for V any Tv can be written as

$$Tv = T(a_1v_1 + \cdots + a_nv_n + b_1u_1 + \cdots + b_mu_m).$$

But each $Tv_k = 0$ and therefore

$$Tv = b_1Tu_1 + \cdots + b_mTu_m.$$

That is, $Tu_1, \dots, Tu_m$ span range(T). It remains to show that $Tu_1, \dots, Tu_m$ are linearly independent. Assume that

$$a_1Tu_1 + \cdots + a_mTu_m = 0.$$

By linearity, this implies that

$$T(a_1u_1 + \cdots + a_mu_m) = 0$$

and so $a_1u_1 + \cdots + a_mu_m \in (T)$. Find $b_1, \dots, b_n$ so that

$$a_1u_1 + \cdots + a_mu_m = b_1v_1 + \cdots + b_nv_n$$

or equivalently,

$$a_1u_1 + \cdots + a_mu_m - b_1v_1 - \cdots - b_nv_n = 0.$$

But $u_1, \dots, u_m, v_1, \dots, v_n$ is a basis for V and thus linearly independent. That is, $a_1 = \cdots = a_m = b_1 = \cdots = b_n = 0$.

Reorder the list to $u_1, \dots, u_m, v_1, \dots, v_n$. Note that reordering the list does not change linear independence or the span. Since $Tu_k = 1 \cdot Tu_k$ and $Tv_k = 0$ for each k, the matrix for T with respect to this basis is as desired. □

Problem 6.4: S12.LA2

Let V be a finite dimensional vector space. A linear transformation $T : V \to V$ is a projection when $T = T^2$. Prove that there exists a basis for V such that the matrix for T with respect to this basis is a diagonal matrix with diagonal entries all zeros or ones.

Proof. Since $T = T^2$, $V = \text{null}(T) \oplus \text{range}(T)$ (see 6.5). Let $v_1, \dots, v_n$ be a basis for null(T) and extend this list to $v_1, \dots, v_n, w_1, \dots, w_m$ to obtain a basis for V. Then $Tw_1, \dots, Tw_m$ is a basis for range(T). Since $V = \text{null}(T) \oplus \text{range}(T)$, the list $v_1, \dots, v_n, Tw_1, \dots, Tw_m$ form a basis for V. With respect to this basis, the matrix for T is as desired. □

Technically there are some more details to prove here, such as linear independence of $Tw_1, \dots, Tw_m$, but this is all routine.

Problem 6.5: S20.LA4

Let V be a finite dimensional vector space and $T : V \to V$ a linear map such that $T^2 = T$.

(a) Prove that $V = T(V) \oplus \ker(T)$.

(b) If $S : V \to V$ is another linear map and $S^2 = S$, $S(V) = T(V)$, and $\ker(S) = \ker(T)$, prove that $S = T$.

Proof. Let $v \in V$. Observe that $v = Tv + (v - Tv)$. Clearly $Tv \in T(V)$ and since $T(v - Tv) = Tv - T^2v = 0$, $v - Tv \in \ker(T)$. Therefore, $V = T(V) + \ker(T)$. To see that this sum is actually a direct sum, it suffices to show that $T(V) \cap \ker(T) = \{0\}$. Let $v \in T(V) \cap \ker(T)$. Then, $Tv = 0$ and $v = Tw$ for some $w \in V$. Together, this means that

$$0 = Tv = T^2w = Tw = v$$

meaning the intersection is trivial. □

Proof. Let $v \in V$. Since $V = S(V) \oplus \ker(S)$, we may write $v = Su + w$ where $w \in \ker(S)$. But, $Su \in S(V) = T(V)$ means that there exists $u' \in V$ such that $Su = Tu'$. Also, $\ker(S) = \ker(T)$ implies that $Tw = 0$. Therefore,

$$Sv = S(Su + w) = S^2u + Sw = Su = Tu' = T^2u' + Tw = T(Su + w) = Tv.$$

As this holds for each $v \in V$, $S = T$. □

Problem 6.6: S20.LA3

Let V be a finite-dimensional vector space and $S, T : V \to V$ linear transformations.

(a) Prove that $\text{rank(S + T)} \leq \text{rank(S)} + \text{rank(T)}$

(b) Prove that $\text{rank(ST)} \leq \max(\text{rank(S)}, \text{rank(T)})$.

Proof. Recall that for any two subspaces U_1, U_2 of a finite dimensional vector space V,

$$\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2).$$

As the dimension is always non-negative, $\dim(U_1 + U_2) \leq \dim(U_1) + \dim(U_2)$. By the linearity of S and T, for any $v \in V$,

$$(S + T)v = Sv + Tv.$$

Therefore, $\text{range}(S + T) = \text{range}(S) + \text{range}(T)$. This means that

$$\text{rank(S + T)} = \dim(\text{range(S)} + \text{range(T)}) \leq \dim(\text{range(S)}) + \dim(\text{range(T)}) = \text{rank(S)} + \text{rank(T)},$$

as desired. □

Proof. For any $v \in V$, $STv = S(Tv)$ and therefore $\text{range}(ST) \subseteq \text{range}(S)$. Since the dimension of a subspace is bounded above by the dimension of the larger space,

$$\text{rank(ST)} = \dim(\text{range(ST)}) \leq \dim(\text{range(S)}) = \text{rank(S)} \leq \max\{\text{rank(S)}, \text{rank(T)}\}.$$

□

Problem 6.7: S19.LA4

Let V be the vector space of all 2×2 matrices and let

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Let $T : V \to V$ be given by $T(B) = AB + BA$.

(a) Prove that T is a linear map.

(b) Compute $T(B)$ when $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(c) Find the eigenvalues and corresponding eigenspaces of T.

Proof. Let $B, C \in V$ and $\alpha \in \mathbb{R}$. Following from properties of matrix multiplication and addition,

$$T(B+C) = A(B+C) + (B+C)A = AB + AC + BA + CA = T(B) + T(C).$$

Likewise,

$$T(\alpha B) = A(\alpha B) + (\alpha B)A = \alpha(AB + BA) = \alpha T(B).$$

□

Solution.

$$T\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} 2a & 2b \\ 3c & 3d \end{pmatrix}.$$

Solution. Notice that V is dimension 4 and so the sum of the dimensions of the eigenspaces is at most 4. Upon inspection, we find that $\lambda = 2$ is an eigenvalue with an eigenspace basis given by $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right\}$. Similarly, $\lambda = 3$ is an eigenvalue with eigenspace basis given by $\left\{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

Problem 6.8: F16.LA1, F14.LA1

Suppose that $T : U \to V$ is a linear transformation with U and V both finite-dimensional vector spaces. Prove that

$$\dim(\ker(T)) + \dim(\text{range(T)}) = \dim(\text{U}).$$

Proof. Suppose that $\dim(U)$ and $\dim(V)$ are both finite. In particular, any subspace of U and V is also finite dimensional. Let $\{v_1, \ldots, v_m\}$ be a basis for $\ker(T) \subseteq U$. Extend this collection to a basis $\beta = \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$ of U. With this chosen basis, it follows that $\dim(\ker(T)) = m$ and $\dim(U) = m + n$. Thus we must show that $\dim(\text{range}(T)) = n$.

Let Tu be an arbitrary element of range(T). Since β is a basis for U, there exist scalars $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ such that

$$u = a_1v_1 + \cdots + a_mv_m + b_1w_1 + \cdots + b_nw_n.$$

By the linearity of T, this means that

$$Tu = a_1Tv_1 + \cdots + a_mTv_m + b_1Tw_1 + \cdots + b_nTw_n = b_1Tw_1 + \cdots + b_nTw_n.$$

The second equality follows as each $v_i \in \ker(T)$ and therefore $a_iTv_i = 0$. This means that $\{Tw_1, \ldots, Tw_n\}$ span range(T).

To see that $\{Tw_1, \ldots, Tw_n\}$ is a linearly independent set, suppose that

$$c_1Tw_1 + \cdots + c_nTw_n = 0.$$

By linearity,

$$T(c_1w_1 + \cdots + c_nw_n) = 0$$

and so $c_1w_1 + \cdots + c_nw_n \in \ker(T)$. Choose scalars $d_1, \ldots, d_m$ such that

$$c_1w_1 + \cdots + c_nw_n = d_1v_1 + \cdots + d_mv_m.$$

Rearranging,

$$c_1w_1 + \cdots + c_nw_n - d_1v_1 - \cdots - d_mv_m = 0.$$

But, β is a basis and so the collection of elements in β is linearly independent. That is, $c_1 = \cdots = c_n = d_1 = \cdots = d_m = 0$. Therefore, $\{Tw_1, \ldots, Tw_n\}$ are linearly independent. As this is a linearly independent spanning set for range(T), $\dim(\text{range}(T)) = n$ as desired. □

Problem 6.9: F12.LA2

Suppose that $V = X \oplus Y$ and define the projection $V \to X$ by $\alpha(v) = x$ where $v = x + y$.

(a) Prove that a necessary and sufficient condition for an endomorphism $T : V \to V$ to be a projection is that $T^2 = T$. Identify X and Y in the case that this condition is satisfied.

(b) Prove that projections T_1 and T_2 have the same range if and only if $T_1T_2 = T_2$ and $T_2T_1 = T_1$.

Proof. Suppose first that $T : V \to V$ is a projection map. That is, for any $v = x + y \in X \oplus Y = V$, $Tv = x$. Then,

$$T^2v = T(T(x + y)) = T(x) = x = T(x + y) = Tv$$

and therefore $T^2 = T$.

Now assume that $T^2 = T$. Let $v \in V$. Observe that $v = (v - Tv) + Tv$. Applying T to both sides yields the following set of equalities:

$$Tv = T(v - Tv) + T^2v = T(v - Tv) + Tv$$

implying that $T(v-Tv) = 0$ and therefore $v-Tv \in \text{range}(T)$. Because $Tv \in \text{range}(T)$, $v \in \text{null}(T)+\text{range}(T)$.

To show that $\text{null}(T) + \text{range}(T)$ is a direct sum, suppose that $0 = x + Tu \in \text{null}(T) + \text{range}(T)$. Then,

$$0 = T(0) = Tx + T^2u = 0 + Tu = Tu$$

and therefore $x = 0$ as well. Since $x = Tu = 0$, $\text{null}(T) + \text{range}(T)$ is a direct sum. That is, $V = \text{range}(T) \oplus \text{null}(T)$.

Since $Tv \in \text{range}(T)$ for any $v \in V$, T is indeed a projection. □

Proof. Suppose that $\text{range}(T_1) = W = \text{range}(T_2)$ with both T_1 and T_2 projections. Let $v \in V$ and suppose that $v = w + w'$ where $w \in W$. Then,

$$T_1T_2v = T_1w = w = T_2v$$

and similarly,

$$T_2T_1v = T_2w = w = T_1v.$$

Assume now that $T_1T_2 = T_2$ and $T_2T_1 = T_1$. Let $v \in V$ and consider $T_1v \in \text{range}(T_1)$. Then,

$$T_1v = T_2T_1v \in \text{range}(T_2).$$

Similarly,

$$T_2v = T_1T_2v \in \text{range}(T_1)$$

implying that $\text{range}(T_1) = \text{range}(T_2)$. □

6.2 Characteristic and Minimal Polynomials

Problem 6.10: (F04.L1)

Let V be a four-dimensional vector space over $\mathbb{R}$ with basis $\{v_1, v_2, v_3, v_4\}$ and let $T : V \to V$ be a linear transformation such that

$$T(v_1) = v_2 \quad T(v_2) = v_3 \quad T(v_3) = v_4 \quad T(v_4) = -v_1 - 4v_2 - 6v_3 - 4fv_4.$$

(a) What is the characteristic polynomial of T?

(b) Is T diagonalizable over $\mathbb{C}$?

Solution. Consider the matrix representation of T with respect to the given basis:

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & -4 \end{pmatrix}.$$

Observe that with respect to this basis, the matrix of T is in rational canonical form with one 4×4 block. From the last column of this matrix, it follows that the minimal polynomial of T is

$$m(x) = x^4 + 4x^3 + 6x^2 + 4x + 1.$$

The characteristic polynomial $c(x)$ of T is a monic, degree-4 polynomial. Furthermore, m must divide c and m and c have the same roots (disregarding multiplicity). This implies that $c(x) = m(x) = (x+1)^4$

Claim: T is not diagonalizable over $\mathbb{C}$.

Proof. The minimal and characteristic polynomials of T are both $(x+1)^4$. Since the minimal polynomial has repeated roots, T is not diagonalizable.

Problem 6.11: (F20.LA2)

Prove or give a counter example.

(a) If a 4×4 real matrix has characteristic polynomial $x^4 - 1$ then its minimal polynomial cannot be $x^2 - 1$.

(b) Every $n \times n$ real matrix is similar over the reals to an upper triangular matrix.

Proof. Notice that $x^4 - 1$ has four distinct roots, namely $\pm 1, \pm i$. Since $x^2 - 1$ has roots ± 1 and the characteristic polynomial divides some power of the minimal polynomial, it is impossible for $x^2 - 1$ to be the minimal polynomial. □

Solution. This is false: consider the matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This matrix has no eigenvalues over the reals. If A were to be similar to an upper triangular matrix, the (1,1) entry would need to correspond to an eigenvalue which is impossible.

Problem 6.12: (F14.LA2)

Prove or provide a counterexample: the characteristic polynomial of a matrix with entries in a field K must be irreducible in the ring $K[x]$.

Solution. This is false. Let $K = \mathbb{R}$ and consider the matrix

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

The characteristic polynomial of A is $(x-1)^2$ which is clearly reducible over $\mathbb{R}[x]$.

6.3 Inner Products

Problem 6.13: (F04.L2)

Let V be a finite dimensional inner product space over $\mathbb{R}$ and $W \subseteq V$ a subspace. Show that:

(a) $V = W + W^{\perp}$.

(b) $W = (W^{\perp})^{\perp}$.

Proof. Let $w_1, \ldots, w_m$ be a basis for W. By applying the Gram-Schmidt process (see 6.14), we may assume this basis is orthonormal. Extend this list to a basis $w_1, \ldots, w_m, v_1, \ldots, v_n$ of V, again without loss of generality assuming the basis is orthonormal.

Claim: The list $v_1, \ldots, v_n$ is a basis for $W^{\perp}$.

Proof. By construction, the list $v_1, \ldots, v_n$ is linearly independent and thus it suffices to prove that this list spans $W^{\perp}$. Let $u \in W^{\perp}$. Since $w_1, \ldots, w_m, v_1, \ldots, v_n$ is a basis of V, write

$$u = a_1 w_1 + \cdots + a_m w_m + b_1 v_1 + \cdots + b_n v_n.$$

Since $u \in W^{\perp}$, for each $j = 1, \ldots, m$, $\langle u, w_j \rangle = 0$. But, the list $w_1, \ldots, w_m, v_1, \ldots, v_n$ is orthonormal and therefore,

$$0 = \langle u, w_j \rangle = a_1 \langle w_1, w_j \rangle + \cdots + a_m \langle w_m, w_j \rangle + b_1 \langle v_1, w_j \rangle + \cdots + b_n \langle v_n, w_j \rangle = a_j \langle w_j, w_j \rangle = a_j.$$

That is,

$$u = b_1 v_1 + \cdots + b_n v_n,$$

proving that $W^{\perp} = \operatorname{span}\{v_1, \ldots, v_n\}$.

From the claim, it follows that $V = W + W^{\perp}$. By construction, $W \cap \operatorname{span}\{v_1, \ldots, v_n\} = \{0\}$ and thus $V = W + W^{\perp} = W \oplus W^{\perp}$, as desired. □

Proof. Let $w \in W$ be arbitrary. For each $u \in W^{\perp}$, $\langle u, w \rangle = 0$. Therefore, $w \in (W^{\perp})^{\perp}$. On the other hand, suppose that $w \in (W^{\perp})^{\perp}$. Then $\langle w, u \rangle = 0$ for each $u \in W^{\perp}$. □

Problem 6.14: (S18.LA2)

Let $V = \mathbb{R}^n$ with the Euclidean inner product. Let $U \subseteq V$ be a subspace.

(a) Prove that U has an orthonormal basis.

(b) Find an orthonormal basis for the space of $(1, 1, 0)$ and $(1, 2, 3)$ inside $\mathbb{R}^3$.

Proof. Any subspace has a basis. Therefore, let $u_1, \ldots, u_m$ be a basis for U. Let $v_1 = u_1$. Next define

$$v_2 = u_2 - \frac{\langle v_1, u_2 \rangle}{||v_1||} v_1.$$

Observe:

$$\langle v_1, v_2 \rangle = \langle v_1, u_2 \rangle - \frac{\langle v_1, u_2 \rangle}{\langle v_1, v_1 \rangle} \langle v_1, v_1 \rangle = 0$$

following directly from the linearity properties of the inner product. For each $j = 2, \ldots, m$, define

$$v_j = u_j - \sum_{k=1}^{j-1} \frac{\langle v_k, u_j \rangle}{||v_k||} v_k.$$

Claim: For any $1 \leq i < j \leq m$, $\langle v_i, v_j \rangle = 0$.

Proof. For the base case, notice that $\langle v_1, v_2 \rangle = 0$. Assume now that whenever $1 \leq i < j < k$, $\langle v_i, v_j \rangle = 0$. Now for any $i = 1, \ldots, k-1$,

$$\begin{aligned}
\langle v_k, v_i \rangle &= \langle u_k - \sum_{j=1}^{i-1} \frac{\langle v_j, u_k \rangle}{||v_j||} v_j, v_i \rangle \\
&= \langle u_k, v_i \rangle - \sum_{j=1}^{i-1} \frac{\langle v_j, u_k \rangle}{||v_j||} \langle v_j, v_i \rangle \\
&= \langle u_k, v_i \rangle - \frac{\langle v_i, u_k \rangle}{||v_i||} \langle v_i, v_i \rangle \\
&= 0
\end{aligned}$$

Line (**??**) follows from the inductive hypothesis since $i, j < k$.

Claim: The list $v_1, \ldots, v_n$ is linearly independent.

Proof. Assume that

$$a_1 v_1 + \cdots + a_n v_n = 0$$

for some constants $a_1, \ldots, a_n$. Notice that each v_j is a linear combination of $u_1, \ldots, u_j$. By rewriting the equation in terms of the u_j and using the fact that $u_1, \ldots, u_n$ are linearly independent, it follows that $a_1 = \cdots = a_n = 0$.

Next define $e_j = \frac{1}{||v_j||} v_j$ for each $j = 1, \ldots, m$. Then each e_j has norm 1, the list $e_1, \ldots, e_m$ is pair-wise orthogonal, and is linearly independent. A linearly independent list of n vectors in an n-dimensional space forms a basis, proving that $e_1, \ldots, e_n$ is as desired. □

Solution. Let $u_1 = (1, 1, 0)$ and $u_2 = (1, 2, 3)$. Using the formulas as defined in the previous proof, let $v_1 = u_1$ and $v_2 = u_2 - \frac{\langle v_1, u_2 \rangle}{||v_1||} v_1 = (-1/2, 1/2, 3/2)$. Normalizing each of these vectors, we obtain an orthonormal basis:

$$\left\{ \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{pmatrix}, \begin{pmatrix} -\sqrt{11}/8 \\ \sqrt{11}/8 \\ 3\sqrt{11}/8 \end{pmatrix} \right\}.$$

Problem 6.15: S19.LA4

Let V be a finite dimensional inner product space over $\mathbb{R}$. If A and B are subspaces of V, prove that $(A + B)^\perp = A^\perp \cap B^\perp$.

Proof. Suppose that $v \in (A + B)^\perp$ and let $a \in A$ be arbitrary. Then, $a + 0 \in A + B$ and therefore,

$$\langle a, v \rangle = \langle a + 0, v \rangle = 0$$

since $\langle a + b, v \rangle = 0$ for all $a + b \in A + B$. Similarly, $\langle b, v \rangle = 0$ for any $b \in B$. Thus $v \in A^\perp \cap B^\perp$.

Now assume that $v \in A^\perp \cap B^\perp$. Let $a + b \in A + B$ be arbitrary. By the linearity of the inner product,

$$\langle a + b, v \rangle = \langle a, v \rangle + \langle b, v \rangle = 0 + 0 = 0$$

proving that $v \in (A + B)^\perp$. □

Problem 6.16: F12.LA1

Let V be the vector space of real $n \times n$ matrices. Show that

$$\langle A, B\rangle = n\text{tr}(AB) - \text{tr}(A)\text{tr}(B)$$

defines a symmetric bilinear form on V.

(a) Prove that $\langle , \rangle$ is singular.

(b) Prove that the restriction of $\langle , \rangle$ to the subspace W of symmetric matrices with 0 trace is positive definite.

Proof. Note that for any $n \times n$ real matrices A and B, $\text{tr}(AB) = \text{tr}(BA)$ and $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$. Furthermore, whenever $\alpha \in \mathbb{R}$, $\text{tr}(\alpha A) = \alpha\text{tr}(A)$. Therefore,

$$\langle A, B\rangle = n\text{tr}(AB) - \text{tr}(A)\text{tr}(B) = n\text{tr}(BA) - \text{tr}(B)\text{tr}(A) = \langle B, A\rangle$$

meaning that $\langle \cdot, \cdot \rangle$ is symmetric. Since

$$\begin{aligned}\langle A, \alpha B + \beta C\rangle &= n\text{tr}(A(\alpha B + \beta C)) - \text{tr}(A)\text{tr}(\alpha B + \beta C)\\ &= n\text{tr}(\alpha AB + \beta AC) - \text{tr}(A)\text{tr}(\alpha B + \beta C)\\ &= \alpha n\text{tr}(AB) + \beta n\text{tr}(AC) - \alpha\text{tr}(A)\text{tr}(B) - \beta\text{tr}(A)\text{tr}(C)\\ &= \alpha\langle A, B\rangle + \beta\langle A, C\rangle\end{aligned}$$

it follows that $\langle \cdot, \cdot \rangle$ is a bilinear form. □

Proof. Let I be the $n \times n$ identity matrix and observe that for any nonzero $n \times n$ matrix B,

$$\langle I, B\rangle = n\text{tr}(IB) - \text{tr}(I)\text{tr}(B) = n\text{tr}(B) - n\text{tr}(B) = 0.$$

Since $I \neq 0$ and B was arbitrary, $\langle \cdot, \cdot \rangle$ is singular. □

Proof. Let $W = \{A_{n\times n} : A \text{ is symmetric and } \text{tr}(A) = 0\}$. Then,

$$\langle A, A, =\rangle n\text{tr}(A^2) - \text{tr}(A)\text{tr}(A) = n\text{tr}(A^2)$$

whenever $A \in W$. Suppose that $A = (a_{ij})$ where a_{ij} denotes the (i, j) entry of A with $1 \leq i, j \leq n$. Because A is symmetric, $a_{ij} = a_{ji}$. Therefore the (i, i) entry of A^2 is

$$b_i = a_{i1}a_{1i} + \cdots + a_{in}a_{ni} = \sum_{j=1}^{n} a_{ij}^2.$$

Thus, the trace of A^2 can be written as $\text{tr}(A^2) = \sum_{i=1}^{n} b_i = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2$. As each term in the sum is at least zero, $\langle A, A\rangle = \text{tr}(A^2) \geq 0$. If $\langle A, A\rangle = 0$, then $\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2 = \text{tr}(A^2) = 0$. As each term in the sum is non-negative, each term must then equal zero. That is, $a_ij = 0$ for $i, j = 1, \ldots, n$ and therefore $A = 0$. □

Problem 6.17: F14

Let U be a real inner-product space and $T : U \to U$ a linear operator on U. Prove that T is an orthogonal linear transformation if and only if $||T(u)|| = ||u||$ for all $u \in U$.

T is an orthogonal linear transformation if $\langle u, v\rangle = \langle Tu, Tv\rangle$.

Proof. Assume first that T is an orthogonal linear transformation. For any $u \in U$,

$$\langle u, u\rangle = ||u||^2 = ||Tu||^2 = \langle Tu, Tu, .\rangle$$

Conversely, assume that $||T(u)|| = ||u||$ for all $u \in U$. Notice that this implies $\langle Tu, Tu\rangle = \langle u, u\rangle$ for each $u \in U$. Let $x, y \in U$ be arbitrary. Then,

$$\langle x+y, x+y\rangle = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle = \langle Tx, Tx\rangle + 2\langle x, y\rangle + \langle Ty, Ty\rangle.$$

On the other hand,

$$\langle T(x+y), T(x+y)\rangle = \langle Tx+Ty, Tx+Ty\rangle = \langle Tx, Tx\rangle + 2\langle Tx, Ty\rangle + \langle Ty, Ty\rangle.$$

Since $||x+y|| = ||T(x+y)||$, we may equate the right sides of the above equations to find that $\langle Tx, Ty\rangle = \langle x, y\rangle$. □

6.4 Canonical Forms

Problem 6.18: S19.LA2

Determine a necessary and sufficient condition for when a matrix $A \in M_2(\mathbb{C})$ has a square root. That is, for which $A \in M_2(\mathbb{C})$ does there exist $B \in M_2(\mathbb{C})$ such that $A = B^2$?

Proof. Since we are working over a complex vector space, A has a normal Jordan form. That is, there exists a block diagonal matrix J with each block a Jordan block and an invertible matrix P such that $A = PJP^{-1}$. If there exists $B \in M_2(\mathbb{C})$ such that $B^2 = J$, then $(PBP^{-1})^2 = A$. On the other hand, if $A = B^2$ then $J = (P^{-1}BP)^2$. Therefore, to determine when A has a square root, it suffices to determine when the Jordan normal form of A has a square root.

Let $p(x)$ be the characteristic polynomial of A. As A is a 2×2 matrix, $\deg(p) = 2$. Note that since J is 2×2, the only possible forms for J are $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ or $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ where $\lambda_1 \neq \lambda_2$.

If $p(x) = (x-\lambda)^2$, then $J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. If $\lambda = 0$, then it is impossible to find a matrix B such that $B^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. If $\lambda \neq 0$, then the matrix $B = \begin{pmatrix} \pm\sqrt{\lambda} & \frac{\pm 1}{2\sqrt{\lambda}} \\ 0 & \pm\sqrt{\lambda} \end{pmatrix}$ is such that $B^2 = J$.

If $p(x) = (x-\lambda_1)(x-\lambda_2)$ for some $\lambda_1 \neq \lambda_2$ then $J = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Letting $B = \begin{pmatrix} \pm\sqrt{\lambda_1} & 0 \\ 0 & \pm\sqrt{\lambda_2} \end{pmatrix}$, we see that $B^2 = J$.

From the above, we conclude that a nonzero matrix A has a square root if and only if zero is not an eigenvalue with multiplicity two. If $A = 0$, then clearly $B = 0$ satisfies $B^2 = A$. □

6.5 Eigenvalues and Eigenvectors

Test text

7 Unfinished

7.1 Spring 2013

Problem 7.1: S13

Fix a prime p and let A, A_1, A_2, and B be finite abelian p-groups.

(a) Assume that A and B are cyclic and that the number of elements of order at most p^r in A equals the corresponding number in B for each $r \in \mathbb{N}$. Show that $A \cong B$.

(b) Suppose that $A = A_1 \oplus A_2$. Show that for any $r \in \mathbb{N}$ the number of elements of order at most p^r in A equals $n_1 \cdot n_2$ where n_i is the number of elements of order at most p^r in A_i.

(c) Prove that A is isomorphic to B if for each $r \in \mathbb{N}$ the number of elements of order at most p^r in A equals the number of elements of order at most p^r in B. *You may use without proof the Fundamental Theorem for Finite Abelian Groups. What does the number of elements of order at most p in A tell you about the number of nontrivial cyclic direct summands of A?*

Problem 7.2: S13

Let $X = \{1, \ldots, n\}$. For any $\tau \in S_n$, the *support* of τ is the set $\{i \in X : \tau(i) \neq i\}$. Let $\sigma \in S_n$ be nontrivial and consider the equivalence relation on X given by $a \sim b$ if and only if there exists $m \in \mathbb{Z}$ where $\sigma^m(a) = b$.

(a) Let $X_0 \subseteq X$ be some equivalence class. Show that the restriction of σ to X_0 is a cyclic permutation of X_0.

(b) Prove that σ is a product of cycles $\sigma_1, \ldots, \sigma_r$ with pairwise disjoint supports.

(c) Show that the order of σ in S_n equals the least common multiple of the cardinalities of the supports of the σ_i.

Problem 7.3: S13

Let G be a finite group and H a proper subgroup of G such that $|G|$ does not divide $[G : H]!$. Prove that H contains a nontrivial normal subgroup of G.

Problem 7.4: S13

(a) Partition the following algebras over $\mathbb{Q}$ into classes of pairwise disjoint isomorphic algebras. Provide full reasoning.

$M_3(\mathbb{Q})$ $\quad \mathbb{Q}[x]/(x^9 - 1)$ $\quad \mathbb{Q}[x]/(x^9 + 6x^2 - 3)$ $\quad \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(x^8 + x^7 + \cdots + x + 1)$

(b) Which of the algebras above are fields?

Problem 7.5: S13

Prove the following case of Eisenstein's irreducibility criterion: Suppose that $f = x^n + \sum_{i=0}^{n-1} a_i x^i$ is a polynomial in $\mathbb{Z}[x]$ of positive degree n and $p \in \mathbb{N}$ is a prime such that p divides a_i for $0 \leq i \leq n-1$ but p^2 does not divide a_0. Then, f is irreducible over $\mathbb{Z}$.

Problem 7.6: S13

Give examples of polynomials in $\mathbb{Q}[x]$ whose splitting fields over $\mathbb{Q}$ have Galois groups over $\mathbb{Q}$ as specified:

(a) The Galois group is isomorphic to S_3.

(b) The Galois group is cyclic of order 6.

Problem 7.7: S13

Let A be an $n \times n$ matrix over $\mathbb{C}$.

(a) State the theorem addressing existence and (qualified) uniqueness of a Jordan canonical form of A.

(b) Show that A is nilpotent if and only if all eigenvalues of A are zero.

(c) Give all possible similarity classes of matrices $A \in M_6(\mathbb{C})$ in Jordan form which satisfy the condition that $A^4 = 0$ but $A^3 \neq 0$.

Problem 7.8: S13

(a) Suppose that V is an n-dimensional vector space over a field F and $\{b_1, \ldots, b_n\}$ is a basis for V. Let $T : V \to V$ be a linear transformation. Show that T is an isomorphism if and only if the set $\{T(b_1), \ldots, T(b_n)\}$ is a basis for V.

(b) Let $A \in M_n(F)$. Deduce from (a) that A is invertible if and only if the columns of A form a basis for the space F^n of $n \times 1$ column vectors over F.

(c) Given a finite field F with q elements, determine the order of the group $GL_2(F)$ of all invertible 2×2 matrices over F.

Problem 7.9: S13

The group S_3 has exactly three conjugacy classes: $\{(1)\}$, $\{(1,2,3),(1,3,2)\}$, and the set of transpositions. Let V be the vector space over $\mathbb{C}$ consisting of all functions $f : S_3 \to \mathbb{C}$ which are constant on the conjugacy classes.

(a) Show that $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ given by

$$\langle f, g \rangle = \frac{1}{6} \sum_{x,y \in S_3} f(x)\overline{g(y)}$$

is a Hermitian inner product on V. Verify that $f_1 = 1$ and $f_2 = \text{sgn}$ in V are orthogonal and each of norm 1.

(b) Extend $\{f_1, f_2\}$ to an orthonormal basis for V.

7.2 Fall 2012

Problem 7.10: F12

(a) Let ν be a primitive 10th root of unity. Compute the Galois group of $\mathbb{Q}(\nu)$.

(b) let $K_t = \mathbb{Q}(\omega)$ where ω is a primitive tth root of unity. Show that $\sqrt[3]{2}$ is not in any K_t.

Problem 7.11: F12

Suppose that R, S, A are all commutative rings with unity.

(a) Suppose that R is a PID, S is an integral domain, and $\varphi : R \to S$ is a surjection. Prove that either φ is an isomorphism or S is a field.

(b) Prove that $A[x]$ is a PID if and only if A is a field.

Problem 7.12: F12

Let M be a 5×5 matrix with rational entries whose characteristic polynomial is of the form

$$(x^2 + 1)(x^3 + x + q).$$

For which, if any, $q \in \mathbb{Q}$ is it possible that there does not exist an invertible matrix A with rational entries such that $A^{-1}MA$ has block diagonal form with a 2×2 block and a 3×3 block?

7.3 Spring 2012

Problem 7.13: S12

(a) State the Sylow Theorems.

(b) Prove that every group of order 126 has a normal subgroup of order 7.

(c) Prove that any group of order 1000 is not simple.

Problem 7.14: S12

Prove or disprove:

(a) If R is an integral domain, then $R[x]$ is an integral domain.

(b) If R is a principal ideal domain, then $R[x]$ is a principal ideal domain.

Problem 7.15: S12

Let F be a finite field.

(a) Show that the multiplicative group F^* is cyclic.

(b) Suppose $|F| = 125 = 5^3$ and $\langle \alpha \rangle = F^*$. What is α^{62}?

(c) Is there a $\beta \neq \alpha$ in F such that $\langle \beta \rangle = F^*$?

Proof. This is a subset of the problem 5.16. The other problem shows that any finite subgroup of the multiplicative group of a field is cyclic (not just when the field itself is finite). □

Problem 7.16: S12

Let $\alpha = \sqrt{-1+\sqrt{2}}$.

(a) Prove that α is the root of a monic polynomial in $\mathbb{Q}[x]$.

(b) Let K be the smallest Galois extension of $\mathbb{Q}$ that contains α. Find the degree $[K:\mathbb{Q}]$.

Problem 7.17: S12

Consider a real vector space $V = \mathbb{R}^n$ with the Euclidean inner product and let U be a subspace of V.

(a) Prove that U has an orthonormal basis. Note that this is the real version of the Gram-Schmidt Theorem.

(b) Find an orthonormal basis for the span of $(1,2,0)$ and $(1,1,3)$ in $\mathbb{R}^3$.

Problem 7.18: S12

Let V be a finite dimensional vector space over $\mathbb{C}$.

(a) Define the characteristic polynomial of a linear transformation of V and the minimal polynomial of a linear transformation of V.

(b) Give an example of two linear transformations $S, T : V \to V$ such that S and T have the same characteristic polynomial, but are not similar.

(c) Give an example of two linear transformations $S, T : V \to V$ such that S and T have the same minimal polynomial, but are not similar.

The characteristic polynomial of a linear transformation $T : V \to V$ is $(x-\lambda_1)^{\ell_1} \cdots (x-\lambda_m)^{\ell_m}$ where $\lambda_1, \ldots, \lambda_j$ are the distinct eigenvalues of T and ℓ_j is the multiplicity of the eigenvalue λ_j. The minimal polynomial of T is the smallest degree monic polynomial p such that $p(T) = 0$.

The minimal polynomial and characteristic polynomial have the same roots, ignoring multiplicity. The minimal polynomial divides the characteristic polynomial.

7.4 Fall 2013

Problem 7.19: F13

(a) Let G be a finite group and H a subgroup of G. Prove that the order of H divides the order of G.

(b) Let $\mathbb{Q}$ and $\mathbb{Z}$ denote the additive groups of the rationals and integers, respectively. Prove that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index.

Problem 7.20: F13

Let $V = \mathbb{R}^2$, regarded as a two-dimensional subspace over $\mathbb{R}$. Let $L(V)$ be the ring of all linear transformations from V to V. let $T \in L(V)$ be given by $T(x, y) = (y, -x)$ and define

$$A = \{S \in L(V) : ST = TS\}.$$

(a) Prove that A is a subring of $L(V)$.

(b) To what well-known ring is A isomorphic?

Problem 7.21: F13

(a) Let N be a non-negative integer and $\alpha \in \mathbb{C}$ a primitive Nth root of unity. FOr which N is it true that $\mathbb{Q}(\alpha) = (\alpha + \alpha^{-1})$?

(b) Let K be a field and β an element of the algebraic closure of K. If $[K(3) : K]$ is odd, prove that $K(\beta) = K(\beta + \beta^{-1})$.

Problem 7.22: F13

Let F be a field and $p_1(x), \ldots, p_r(x)$ distinct, monic, irreducible polynomials in $F[x]$. Let $f(x) = p_1(x)^{n_1} + \cdots + p_r(x)^{n_r}$ where each n_i is a positive integer.

(a) Determine the number of ideals in $F[x]/\langle f(x)\rangle$.

(b) Determine the number of prime ideals in $F[x]/\langle f(x)\rangle$.

Problem 7.23: F13

Let V be a finite dimensional vector space of $\mathbb{Q}$ and let M be an automorphism of V such that M fixes no non-zero vector in V. Suppose that M^p is the identity map on V with p a prime. Show that the dimension of V is divisible by $p - 1$. *You may assume that the polynomial $x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.*

Problem 7.24: F13

Let $\mathbb{R}^3$ have the usual inner product and suppose that $(a, b, c) \in \mathbb{R}^3$ is of unit length. Let W be the plane given by $ax + by + cz = 0$. Let ℓ be the line through the origin in the direction (a, b, c).

(a) Define the standard matrix representing the orthogonal projection of $\mathbb{R}^3$ onto ℓ.

(b) Define the standard matrix representing the orthogonal projection of $\mathbb{R}^3$ onto W.

Problem 7.25: F19

Let p be a prime number and suppose that $1 \leq n < p^2$ is an integer. Show that every Sylow p-subgroup of the symmetric group S_n is abelian.

Problem 7.26: F20

Let G be a finite group, $x \in G$, and H a subgroup of G.

(a) Prove that the number of conjugates of x in G divides order(G)/order(x).

(b) Prove that the number of conjugates of H in G divides the index of H in G.

Problem 7.27: S19

State and prove Lagrange's Theorem. Prove that a subgroup of a cyclic group is cyclic.

Problem 7.28: S19

Prove that $\sigma, \tau \in S_n$ are conjugate if and only if for each $m \geq 2$ the number of m-cycles in a cycle decomposition of σ equals the number of m-cycles in a cycle decomposition of τ.

Problem 7.29: F20

Show that any finitely generated group of $(\mathbb{Q}, +)$ is cyclic. Use this to prove that the direct product $(\mathbb{Q}, +) \times (\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

Problem 7.30: S20

Let R be a commutative ring with identity. Show that if p is a prime ideal in R then

$$p(x) = \left\{ \text{all polynomials } \sum_i a_i x^i \text{ with each } a_i \in p \right\}$$

is a prime ideal in $R[x]$.

Problem 7.31: F20

Prove or provide a counter example: Suppose that K is a finite extension of F. $F \subseteq L \subseteq K$, $F \subseteq M \subseteq KL$, $LM = K$ and $L \cap M = F$. Then $[L : F][M : F] = [K : F]$. Here, LM denotes the composition of the fields L and M.

Problem 7.32: F20

(i) Let R be a UFD and d a nonzero element in R. Prove that there are only finitely many principal ideals in R that contain the ideal (d).

(ii) Give an example of a UFD R and a nonzero element $d \in R$ such that there are infinitely many ideals in R that contain (d).

Problem 7.33: F20

It is known that real symmetric matrices are always diagonalizable. You may assume this fact.

(a) What special property do the eigenspaces of a real symmetric matrix have?

(b) Prove that any real symmetric matrix S can be diagonalized by an orthonormal matrix U.

Problem 7.34: F20

Let V be a finite dimensional complex vector space and $T : V \to V$ a linear transformation.

(a) Show that V has a "flag" of subspaces $V_0 = 0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ such that $\dim(V_i) = i$ and $T(V_i) \subseteq V_i$ for each i.

(b) Show that there is a basis for V such that the matrix of T with respect to this basis is upper triangular.

Proof. See 3.3. □