Contents

1 Directory

- **Fall 2021**:
  - G1 Problem 5.3
  - G2 Problem 2.1
  - G3 Problem 15.45
- **Fall 2020**:
  - G1 Problem 15.36
  - G2 Problem 4.6
  - G3 Problem 15.30
  - RF1 Problem 15.39
  - RF2 Problem 15.40
  - RF3 Problem 15.41
  - LA1 Problem 15.42
  - LA2 Problem 15.43
  - LA3 Problem 15.44
- **Fall 2019**: RF1 Problem 7.1
- **Fall 2018**: G1 Problem 6.2
- **Spring 2011**:
  - RF2 Problem 7.2
  - RF3 Problem 10.1
- **Fall 2012**:
  - G1 Problem 4.2
  - G2 Problem 6.1, Problem 5.1
  - G3 Problem 3.3
  - RF1 Problem 15.11
  - RF2 Problem 15.12
  - RF3 Problem 8.2
  - LA1 Problem 13.1
  - LA2 Problem 11.2
  - LA3 Problem 15.13
- **Spring 2012**:
  - G1 Problem 3.2
  - G2 Problem 3.1
  - G3 Problem 15.14
  - RF1 Problem 15.15
  - RF2 Problem 15.16
  - RF3 Problem 15.17
  - LA1 Problem 15.18

  - LA2 Problem 15.19
  - LA3 Problem 15.20

- **Fall 2013**:
  - G1 Problem 3.4
  - G2 Problem 15.21
  - G3 Problem 15.22
  - RF1 Problem 15.23
  - RF2 Problem 15.24
  - RF3 Problem 15.25
  - LA1 Problem 15.26
  - LA2 Problem 15.27
  - LA3 Problem 15.28

- **Spring 2013**:
  - G1 Problem 15.2
  - G2 Problem 15.3
  - G3 Problem 15.4
  - RF1 Problem 15.5
  - RF2 Problem 15.6
  - RF3 Problem 15.7
  - LA1 Problem 15.8
  - LA2 Problem 15.9
  - LA3 Problem 15.10

- **Fall 2014**:
  - G1 Problem 4.4
  - G2 Problem 9.1
  - G3 Problem 4.1
  - RF1 Problem **??**
  - RF2 Problem 15.1
  - RF3 Problem 8.1
  - LA1 Problem 11.1
  - LA2 Problem 12.1
  - LA3 Problem 13.2

2 Properties of Normal Subgroups

Problem 2.1: F21

(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, $\mathrm{im}(\varphi) = G/N$. 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,

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

□

3 General Group Theory

Problem 3.1: 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 $yz \in \{0, 1, \dots, 35\}$. 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 3.2: 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. $\square$

Problem 3.3: F12

(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 $a = bh_1 h_2^{-1}$ and $b = ah_2 h_1^{-1}$. Then, for any $h \in H$,

$$ah = bh_1 h_2^{-1} h \in bH$$

and

$$bh = ah_2 h_1^{-1} h \in aH.$$

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 $g_1 H, \ldots, g_n H$ be the left cosets of H in G. Each $g_i H$ has $|H|$ elements and each $g \in G$ is in some $g_i H$. 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 3.4: F13

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. $\square$

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 The Sylow Theorems

Problem 4.1: 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 4.2: F12

(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. Stuck on how to proceed here! We know that there's an element of order 2, but I don't know how this can be used. □

Problem 4.3: 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 4.4: F19, F14

(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 4.5: 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. $\square$

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. $\square$

Problem 4.6: 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 $\mathbb{Z}_2$. $\square$

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. $\square$

Problem 4.7: 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 $|G/P| = 3$. $\square$

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? $\square$

5 $G/Z(G)$ is Cyclic

Problem 5.1: 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. See 6.1 □

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 5.3). 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 5.2: 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 5.3: F21

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 5.2. □

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 $|H : Z(H)| = 6$.

6 Order Stabilizer Theorem

Problem 6.1: 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 5.1. □

Note that 6.2 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 6.2: F18

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 $x^p = e$. $\square$

7 Ideals

Problem 7.1: F19

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. $\square$

Problem 7.2: 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. $\square$

8 Nilpotent

Problem 8.1: F14

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. $\square$

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. $\square$

Problem 8.2: F12

(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. We show that $\mathbb{Z}/m\mathbb{Z}$ has some non-zero nilpotent element if and only if m has some multiple prime factor. Suppose first that x is a non-zero nilpotent element of $\mathbb{Z}/m\mathbb{Z}$. Then there exists an integer $k \geq 2$ such that $x^k = 0$. That is, x^k divides m. Note that $x \neq 1$ because any power of 1 is 1. Let p be any prime factor of x. Then, p^k divides x^k and therefore p^k divides m. By assumption $k \geq 2$ and thus m has a multiple prime factor.

Conversely, assume that m has some multiple prime factor. That is, there exists a prime p such that p^k divides m with $k \geq 2$. Note that $p \in \mathbb{Z}/m\mathbb{Z}$ and since p^k divides m, $p^k = 0$ in $\mathbb{Z}/m\mathbb{Z}$. Therefore p is a nonzero nilpotent element of $\mathbb{Z}/m\mathbb{Z}$. $\square$

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. $\square$

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. $\square$

9 Finite Fields

Problem 9.1: F14

Prove that the multiplicative group of nohnzero elements of a finite field is cyclic.

Proof. Suppose that F is a finite field and let $K = F^{\times}$ be the multiplicative group of nonzero elements in F. Since F is finite, K is finite – let $|K| = n$. Let $a \in K$ be of maximal order, say m. By Lagrange's Theorem, $m|n$ and $m \leq n$. Suppose now that $b \in K$ is arbitrary and of order r.

> **Claim:** There exists an element $c \in K$ of order $\mathrm{lcm}(r, m)$.
>
> *Proof.* Look for shorter proof of this!.

Then the order of c is $\mathrm{lcm}(r, m) \geq m$. Because m is the maximal order of elements in K, $\mathrm{lcm}(r, m) \leq m$ and therefore $\mathrm{lcm} r, m = m$. Since r divides $\mathrm{lcm} r, m = m$ and b is of order r, it follows that $b^m = 1$. As b was an arbitrary element of K, every element of K is a root of the polynomial $x^m - 1$. This polynomial has at most m roots and therefore $n \leq m$. This implies that $n = m$ and whence K is cyclic and generated by a. □

10 Galois Groups

Problem 10.1: S11.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, $G \cong D_8$. □

11 Linear Maps

Problem 11.1: F14

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 $\{v_1, \dots, v_m\}$ be a basis for $\ker(T) \subseteq U$. Extend this collection to a basis $\beta = \{v_1, \dots, v_m, w_1, \dots, w_n\}$ 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 $a_1, \dots, a_m$ and $b_1, \dots, b_n$ 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 $\{Tw_1, \dots, Tw_n\}$ span range(T).

To see that $\{Tw_1, \dots, Tw_n\}$ 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 $d_1, \dots, d_m$ 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, $\{Tw_1, \dots, Tw_n\}$ are linearly independent. As this is a linearly independent spanning set for range(T), $\dim(\text{range}(T)) = n$ as desired. ☐

Problem 11.2: F12

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:
$$Tv = T(v - Tv) + T^2 v = T(v - Tv) + Tv$$
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,
$$0 = T(0) = Tx + T^2 u = 0 + Tu = Tu$$
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,
$$T_1 T_2 v = T_1 w = w = T_2 v$$
and similarly,
$$T_2 T_1 v = T_2 w = w = T_1 v.$$
Assume now that $T_1 T_2 = T_2$ and $T_2 T_1 = T_1$. Let $v \in V$ and consider $T_1 v \in \text{range}(T_1)$. Then,
$$T_1 v = T_2 T_1 v \in \text{range}(T_2).$$
Similarly,
$$T_2 v = T_1 T_2 v \in \text{range}(T_1)$$
implying that $\text{range}(T_1) = \text{range}(T_2)$. □

12 Characteristic and Minimal Polynomials

Problem 12.1: F14

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 $\mathbb{R}[x]$.

13 Inner Products

Problem 13.1: F12

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

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

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, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ and $\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$. Furthermore, whenever $\alpha \in \mathbb{R}$, $\mathrm{tr}(\alpha A) = \alpha\mathrm{tr}(A)$. Therefore,

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

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

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

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,

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

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

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

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

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 $\mathrm{tr}(A^2) = \sum_{i=1}^n b_i = \sum_{i=1}^n \sum_{j=1}^n a_{ij}^2$. As each term in the sum is at least zero, $\langle A, A\rangle = \mathrm{tr}(A^2) \geq 0$. If $\langle A, A\rangle = 0$, then $\sum_{i=1}^n \sum_{j=1}^n a_{ij}^2 = \mathrm{tr}(A^2) = 0$. 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 13.2: 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 $\langle Tx, Ty\rangle = \langle x, y\rangle$. $\square$

14 Linear Algebra Done Right Problems

14.1 Invariant Subspaces

Linear Algebra Done Right: 5A.1

Suppose that $T \in \mathscr{L}(V)$ and $U \subseteq V$ is a subspace. Prove that if $U \subseteq (T)$ then U is invariant under T. Prove that if $\text{range}(T) \subseteq U$ then U is invariant under T.

Proof. Assume that $U \subseteq (T)$ and $u \in U$. Then, $u \in (T)$ and so $Tu = 0 \in U$. □

Proof. Assume that $\text{range}(T) \subseteq U$ and that $u \in U$. Then, $Tu \in \text{range}(T) \subseteq U$. □

Linear Algebra Done Right: 5A.2

Suppose that $S, T \in \mathscr{L}(V)$ such that $ST = TS$. Prove that (S) is invariant under T.

Proof. Suppose that $u \in (S)$. Then $Su = 0$ implying that $TSu = 0$. By assumption, this means that $STu = 0$ and therefore $Tu \in (S)$. □

Linear Algebra Done Right: 5A.3

Suppose that $S, T \in \mathscr{L}(V)$ such that $ST = TS$. Prove that $\text{range}(S)$ is invariant under T.

Proof. Let $v \in \text{range}(S)$ where $v = Su$ for some $u \in V$. Then,

$$Tv = (TS)u = (ST)u \in \text{range}(S)$$

proving that $\text{range}(S)$ is invariant under T, as desired. □

Linear Algebra Done Right: 5A.4

Suppose that $T \in \mathscr{L}(V)$ and $U_1, \ldots, U_m \subseteq V$ are all subspaces that are invariant under T. Prove that $U_1 + \cdots + U_m$ is invariant under T.

Proof. Take $\sum_{i=1}^m u_i \in U_1 + \cdots + U_m$. As each U_i is invariant under T, each $Tu_i \in U_i$. Therefore,

$$T\left(\sum_{i=1}^m u_i\right) = \sum_{i=1}^m Tu_i \in U_1 + \cdots + U_m$$

as desired. □

Linear Algebra Done Right: 5A.5

Let $T \in \mathscr{L}(V)$. Prove that the intersection of any collection of subspaces of V invariant under T is invariant under T.

Proof. Let $\{U_\alpha\}_{\alpha \in \mathscr{A}}$ be a collection of subspaces of V that are invariant under T. Suppose that $v \in U = \bigcap_{\alpha \in \mathscr{A}} U_\alpha$. Then $v \in U_\alpha$ and thus $Tv \in U_\alpha$ for each $\alpha \in \mathscr{A}$. This implies that $Tv \in U$, as desired. □

Linear Algebra Done Right: 5A.6

If V is a finite-dimensional vector space and U is a subspace of V that is invariant under every $T \in \mathscr{L}(V)$, then $U = \{0\}$ or $U = V$.

Proof. We prove the contrapositive. Suppose that $U \neq \{0\}$ and $U \neq V$. Choose some nonzero $u \in U$ and let $u' \in V - U$. Extend $\{u\}$ to a basis $\{u, v_1, \ldots, v_m\}$ for V. Define $T \in \mathscr{L}(V)$ by $Tu = u'$ and $Tv_k = 0$ for each $k = 1, \ldots, m$. By construction, U is not invariant under T as $Tu \notin U$. □

Linear Algebra Done Right: 5A.7

Suppose that $T \in \mathscr{L}(\mathbb{R}^2)$ is given by $T(x, y) = (-3y, x)$. Find the eigenvalues and eigenvectors of T.

Proof. If λ is an eigenvalue of T then

$$(-3y, x) = T(x, y) = (\lambda x, \lambda y).$$

This implies that $x = \lambda y$ and $-3y = \lambda x$. Therefore, $-3y = \lambda^2 y$. Note that $y \neq 0$ since $y = 0$ implies $x = 0$ and eigenvectors are nonzero. Therefore, $-3 = \lambda^2$ which has no solutions over $\mathbb{R}$. Whence T has no eigenvalues. □

Linear Algebra Done Right: 5A.8

Define $T \in \mathscr{L}(\mathbb{F}^2)$ by

$$T(w, z) = (z, w)$$

and find all eigenvalues and eigenvectors of T.

Proof. Suppose that λ is an eigenvalue of T. Then

$$(z, w) = T(w, z) = (\lambda w, \lambda z)$$

implying that $w = \lambda z$ and $z = \lambda w$. This means that $w = \lambda^2 w$. If $w = 0$ then $z = 0$, meaning that λ has no associated eigenvector. Therefore, $w \neq 0$ and so $\lambda = \pm 1$. When $\lambda = 1$, eigenvectors are of the form (w, w). When $\lambda = -1$, eigenvectors are of the form $(w, -w)$. □

Linear Algebra Done Right: 5A.9

Define $T \in \mathscr{L}(\mathbb{F}^3)$ by

$$T(z_1, z_2, z_3) = (2z_2, 0, 5z_3)$$

and find all eigenvalues and eigenvectors of T.

Proof. Suppose that λ is an eigenvalue of T. Then,

$$(2z_2, 0, 5z_3) = T(z_1, z_2, z_3) = (\lambda z_1, \lambda z_2, \lambda z_3).$$

This means that

$$2z_2 = \lambda z_1 \quad \text{and} \quad 0 = \lambda z_2 \quad \text{and} \quad 5z_3 = \lambda z_3.$$

If $\lambda = 0$, then $z_1 = z_3 = 0$ and z_2 is free. Therefore, $\lambda = 0$ has corresponding eigenvectors of the form $(0, z, 0)$. If $\lambda \neq 0$, $z_2 = 0$ and thus $z_1 = 0$ as well. This means that $z_3 \neq 0$ and therefore $\lambda = 5$. If $\lambda = 5$, then z_3 is free and $z_1 = z_2 = 0$. That is, $\lambda = 5$ has corresponding eigenvectors of the form $(0, 0, z)$. □

Linear Algebra Done Right: 5A.10

Define $T \in \mathscr{L}(\mathbb{F}^n)$ by

$$T(x_1, x_2, \ldots, x_n) = (x_1, 2x_2, \ldots, nx_n).$$

Find the eigenvalues and eigenvectors of T. Find the invariant subspaces of T.

Proof. If λ is an eigenvalue of T, then

$$(x_1, 2x_2, \ldots, nx_n) = T(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$$

resulting in the system of n equations of the form $\lambda x_k = kx_k$ for $k = 1, \ldots, n$. Then $\lambda = k$ is an eigenvalue with eigenvector of the form $(v_1, \ldots, v_n)$ where $v_k = 1$ and $v_j = 0$ when $j \neq k$ for each $k = 1, \ldots, n$. As this accounts of n eigenvalues in an n-dimensional space, these are all possible eigenvalue-eigenvector pairs.

Let these eigenvectors be denoted by $w_1, \ldots, w_n$ where w_k has eigenvalue $\lambda = k$. The span of each w_k is one-dimensional and is an invariant subspace under T. Denote these subspaces by $U_1, \ldots, U_n$.
Second part of this solution is not finished! □

Linear Algebra Done Right: 5A.14

15 Unfinished

15.1 Fall 2014

Problem 15.1: F14

(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.

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

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

Any field that contains $\sqrt{1+\sqrt{2}}$ also contains $-\sqrt{1+\sqrt{2}}$ as fields are closed under additive inverses. The converse of this statement is true as well and an analogous statement holds for $\sqrt{1-\sqrt{2}}$.

Since $x^4 - 2x^2 - 1$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion and has both $\sqrt{1+\sqrt{2}}$ and $\sqrt{1-\sqrt{2}}$ as roots,

$$[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt{1-\sqrt{2}}) : \mathbb{Q}].$$

□

15.2 Spring 2013

Problem 15.2: 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 15.3: 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 15.4: 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 15.5: S13

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

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

(b) Which of the algebras above are fields?

Problem 15.6: 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 15.7: 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 15.8: 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 15.9: 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 15.10: S13

The group S_3 has exactly three conjugacy classews: $\{(1)\}$, $\{(1,2,3),(1,3,2)\}$, 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 $f_2 = \operatorname{sgn}$ in V are orthogonal and each of norm 1.

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

15.3 Fall 2012

Problem 15.11: 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 15.12: 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 15.13: 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?

15.4 Spring 2012

Problem 15.14: 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 15.15: 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 15.16: 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 $\langle \beta \rangle = F^*$?

Problem 15.17: 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 15.18: 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 15.19: S12

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.

Problem 15.20: 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 lienar 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.

15.5 Fall 2013

Problem 15.21: F13

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

Proof. Suppose that G is a finite group of order greater than two. Fix some non-identity element $x \in G$. Define $\varphi : G \to G$ by $\varphi : y \mapsto xyx^{-1}$. Notice that for any $a, b \in G$,

$$\varphi(ab) = xabx^{-1} = (xax^{-1})(xbx^{-1}) = \varphi(a)\varphi(b)$$

proving that φ is a homomorphism. Observe that φ is bijective with inverse given by $y \mapsto x^{-1}yx$. Therefore, φ is an automorphism. □

Problem 15.22: 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 15.23: 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 15.24: 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 15.25: 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 15.26: F13

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.

Problem 15.27: 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 15.28: 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 15.29: 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 15.30: 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 15.31: S20

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

Problem 15.32: S19

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

Problem 15.33: 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.

Problem 15.34: 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 15.35: S20

(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.

Problem 15.36: 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 15.37: 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 15.38: S20

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.

Problem 15.39: F20

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.

Problem 15.40: 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 15.41: 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 15.42: 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 15.43: F20

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.

Problem 15.44: 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.

Problem 15.45: F21

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 subgroupsQ_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 $|M| = pq^2$. □

Problem 15.46: S19

(a) Suppose that G is a group and $G/Z(G)$ is cyclic. Prove that G is abelian.

(b) Let p be a prime number and G a non-cyclic finite p-group. Prove that G contains a normal subgroup N such that $G/N \cong C \oplus C$ where C is a cyclic group of order p.

Proof. See **??**. □

Proof. Suppose that $|G| = p^k$ with $k \geq 2$. Assume that G is not cyclic. □