Contents

1 Directory

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

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

□

3 The Sylow Theorems

Problem 3.1: 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 3.2: 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 3.3: F19

(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 3.4: 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 3.5: 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 3.6: 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 $G/Z(G)$ is Cyclic

Problem 4.1: 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 4.2: 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 4.1. □

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

5 Order Stabilizer Theorem

Note that 5.1 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 5.1: 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 $x^p = e$. □

6 Ideals

Problem 6.1: 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. □

7 Linear Algebra Done Right Problems

7.1 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

8 Unfinished

8.1 Fall 2012

Problem 8.1: 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. Suppose that $Z(G)$ is trivial and consists only of the identity element $e \in G$. If $k = 1$, the order of G is prime which implies that G is cyclic and therefore abelian. Therefore, assume that $k > 1$. □

Problem 8.2: F12

(a) State and prove Lagrange's Theorem.

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

Problem 8.3: 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 8.4: 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 8.5: 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.

Problem 8.6: F12

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.

Problem 8.7: 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 $v = x + y \in V$ be arbitrary. Observe that $T^2x = Tx$ and therefore $x - Tx \in (T)$. □

Problem 8.8: 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?

8.2 Spring 2012

Problem 8.9: S12

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

Problem 8.10: S12

(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 $\mathbb{Z}_4 \times \mathbb{Z}_{36}$.

Problem 8.11: 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 8.12: 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 8.13: 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 8.14: 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 8.15: 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 8.16: 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 8.17: 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.

Problem 8.18: 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 8.19: 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 8.20: S20

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

Problem 8.21: S19

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

Problem 8.22: 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 8.23: 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 8.24: 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 8.25: 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 8.26: 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 8.27: 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 8.28: 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 8.29: 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 8.30: 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 8.31: 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 8.32: 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 8.33: 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 8.34: 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 8.35: 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. □