Algebra Prelim Solutions

Contents

1 Winter 2020

1.1 Linear Algebra

1.1.1 Problem 1

Exercise 1. Let V be an n-dimensional vector space over a field K and let $T\colon V \to V$ be a linear map. We say $v \in V$ is a **cyclic vector** for T if $\{v, Tv, \dots, T^{n-1}v\}$ is a basis for V. Let $\chi_T(X) \in K[X]$ be the characteristic polynomial of T and let $\pi_T(X) \in K[X]$ be the minimal polynomial of T over K. Prove the following:

1. Let $v \in V$ and suppose $T^{n-1}v \neq 0$ but $T^n v = 0$. Then v is a cyclic vector for T.
2. If V has a cyclic vector for T, then $\chi_T = \pi_T$.
3. If T is diagonalizable and $\chi_T = \pi_T$, then V has a cyclic vector for T.
4. If V has a cyclic vector for T and $S\colon V \to V$ is a linear map which commutes with T, then S is a polynomial in T.

Solution 1. 1. We first show $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Suppose we have

$$a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v = 0 \tag{1}$$

for some $a_0, a_1, \dots, a_{n-1} \in K$. Applying T^{n-1} to both sides of (1) gives us $a_0 T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_0 = 0$. Thus (1) becomes

$$a_1 Tv + a_2 T^2 v + \cdots + a_{n-1}T^{n-1}v = 0 \tag{2}$$

Applying T^{n-2} to both sides of (2) gives us $a_1 T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_1 = 0$. Proceeding inductively, we have

$$a_k T^k v + a_{k+1}T^{k+1}v + \cdots + a_{n-1}T^{n-1}v = 0 \tag{3}$$

for some $1 \leq k \leq n-1$. Applying T^{n-1-k} to both sides of (3) gives us $a_k T^{n-1}v = 0$. Since $T^{n-1}v \neq 0$, we must have $a_k = 0$. This implies $a_1 = a_2 = \cdots = a_{n-1} = 0$, and thus $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Finally, observe that $\{v, Tv, \dots, T^{n-1}v\}$ spans V since $\operatorname{span}_K(\{v, Tv, \dots, T^{n-1}v\}) \subseteq V$ and $\dim V = n = \#\{v, Tv, \dots, T^{n-1}v\}$. Therefore $\{v, Tv, \dots, T^{n-1}v\}$ is a basis for V.

2. Let $v \in V$ be a cyclic vector for T. Express the minimal polynomial of T over K as

$$\pi_T(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0,$$

where $1 \leq k \leq n$. As π_T is the minimal polynomial of T over K, we must have

$$T^k v + a_{k-1}T^{k-1}v + \cdots + a_1 T + a_0 = 0. \tag{4}$$

If $k \leq n-1$, then (4) gives a nontrivial relation in $\{v, Tv, \dots, T^{n-1}v\}$, contradicting the fact that $\{v, Tv, \dots, T^{n-1}v\}$ is linearly independent. Thus $k = n$, which implies $\pi_T = \chi_T$ since $\pi_T \mid \chi_T$ and both π_T and χ_T are monic of the same degree.

3. Suppose T is diagonalizable and $\pi_T = \chi_T$. Let $\{v_1, \dots, v_n\}$ be an eigenbasis for T with corresponding eigenvalues $\{\lambda_1, \dots, \lambda_n\}$. Suppose we have

$$a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v = 0 \tag{5}$$

for some $a_0, a_1, \dots, a_{n-1} \in K$. Then we have

$$\begin{aligned} 0 &= a_0 v + a_1 Tv + \cdots + a_{n-1}T^{n-1}v \\ &= \sum_{i=0}^{n-1} a_i \lambda_k^i v \end{aligned}$$

1.1.2 Problem 2

Exercise 2. Let V and W be real vector spaces, and let $\mathrm{Hom}_{\mathbb{R}}(W, V)$ denote the set of linear transformations $W \to V$, which is a real vector space.

1. Let $z \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Define $z\phi \colon \mathbb{C} \to V$ by the formula
$$(z\phi)(w) = \phi(zw) \tag{6}$$
for all $w \in \mathbb{C}$. Prove that $z\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.
2. Prove that $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is a complex vector space using (6) to define scalar multiplication.
3. Prove that if $d = \dim_{\mathbb{R}}(V) < \infty$, then $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.
4. Prove that if $f \colon V \to W$ is a linear transformation over $\mathbb{R}$, then the function $f_* \colon \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, W)$, defined by
$$f_*(\phi) = f \circ \phi$$
for all $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, is a linear transformation over $\mathbb{C}$.
5. Prove that if $\lambda \in \mathbb{R}$ is an eigenvalue for a linear transformation $f \colon V \to V$, then λ is an eigenvalue for $f_* \colon \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

Solution 2. 1. Let $z_1, z_2 \in \mathbb{C}$ and let $a_1, a_2 \in \mathbb{R}$. Then we have
$$\begin{aligned}(z\phi)(a_1z_1 + a_2z_2) &= \phi(z(a_1z_1 + a_2z_2)) \\ &= \phi(a_1zz_1 + a_2zz_2) \\ &= a_1\phi(zz_1) + a_2\phi(zz_2) \\ &= a_1(z\phi)(z_1) + a_2(z\phi)(z_2).\end{aligned}$$
It follows that $z\phi$ is $\mathbb{R}$-linear, and hence $z\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

2. We give $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ a complex vector space structure via the scalar multiplication
$$z \cdot \phi = z\phi$$
for all $z \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, where $z\phi$ is the $\mathbb{R}$-linear map defined in (6). First note that $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is an abelian since it already has the structure of an $\mathbb{R}$-vector space, so we just need to show that $\mathbb{C}$ acts on $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ by additive maps. Clearly $1 \cdot \phi = \phi$ for all $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Let $z_1, z_2 \in \mathbb{C}$ and let $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have
$$\begin{aligned}(z_1 \cdot (z_2 \cdot \phi))(w) &= (z_1(z_2\phi))(w) \\ &= (z_2\phi)(z_1w) \\ &= \phi(z_2z_1w)) \\ &= \phi(z_1z_2w) \\ &= ((z_1z_2)\phi)(w) \\ &= (z_1z_2 \cdot \phi)(w).\end{aligned}$$
It follows that $z_1 \cdot (z_2 \cdot \phi) = z_1z_2 \cdot \phi$.

Next, let $z \in \mathbb{C}$ and let $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have
$$\begin{aligned}(z \cdot (\phi_1 + \phi_2))(w) &= (z(\phi_1 + \phi_2))(w) \\ &= (\phi_1 + \phi_2)(zw) \\ &= \phi_1(zw) + \phi_2(zw) \\ &= (z\phi_1)(w) + (z\phi_2)(w) \\ &= (z \cdot \phi_1)(w) + (z \cdot \phi_2)(w) \\ &= (z \cdot \phi_1 + z \cdot \phi_2)(w).\end{aligned}$$

It follows that $z \cdot (\phi_1 + \phi_2) = z \cdot \phi_1 + z \cdot \phi_2$. A similar calculation also shows that if $z_1, z_2 \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$, then $(z_1 + z_2) \cdot \phi = z_1 \cdot \phi + z_2 \cdot \phi$.

3. Before we prove this, let us prove another result:

Proposition 1.1. *Let L/K be a finite extension of fields and let V be a finite dimensional L-vector space (so V is a K-vector space by restriction of scalars). Then we have*

$$\dim_L V = [L : K] \cdot \dim_K V.$$

Proof. Denote $m = [L : K]$ and denote $n = \dim_K V$. Let $\mathbf{e} = (e_1, \ldots, e_m)$ be an ordered basis for L as a K-vector space, and let $\mathbf{v} = (v_1, \ldots, v_n)$ be an ordered basis for V as an L-vector space. We claim that $\mathbf{e} \otimes \mathbf{v} = (e_1 v_1, \ldots, e_1 v_n, e_2 v_1, \ldots, e_2 v_n, \ldots, e_m v_1, \ldots, e_m v_n)$ is an ordered basis for V as a K-vector space. Indeed, let us first show that $\mathbf{e} \otimes \mathbf{v}$ spans V as a K-vector space. Let $v \in V$. Since $\mathbf{v}$ spans V as a L-vector space, we have

$$v = b_1 v_1 + \cdots + b_n v_n$$

for some $b_1, \ldots, b_n \in L$. Since $\mathbf{e}$ spans L as a K-vector space, for each $1 \leq j \leq n$ we have

$$b_j = a_{1j} e_1 + \cdots + a_{mj} e_m.$$

for some $a_{1j}, \ldots, a_{mj} \in K$. Therefore, we have

$$\begin{aligned} v &= \sum_{j=1}^{n} b_j v_j \\ &= \sum_{i=1}^{n} \left(\sum_{i=1}^{m} a_{ij} e_i \right) v_j \\ &= \sum_{1 \leq i \leq m} a_{ij} e_i v_j. \\ &\quad 1 \leq j \leq n \end{aligned}$$

Therefore $\mathbf{e} \otimes \mathbf{v}$ spans V as K-vector space. Next we show that $\mathbf{e} \otimes \mathbf{v}$ is linearly independent. Suppose we have

$$\sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} a_{ij} e_i v_j = 0$$

for some $a_{ij} \in K$. Since $\mathbf{v}$ is linearly independent, this implies

$$\sum_{i=1}^{m} a_{ij} e_i = 0$$

for each $1 \leq j \leq n$. Since $\mathbf{e}$ is linearly independent, this implies $a_{ij} = 0$ for each $1 \leq i \leq m$ and for each $1 \leq j \leq n$. Thus $\mathbf{e} \otimes \mathbf{v}$ is linearly independent. □

Now we continue with our original problem. First note that as an $\mathbb{R}$-vector space, we have $\dim_{\mathbb{R}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = 2d$. Thus, the proposition above tells us that as $\mathbb{C}$-dimensional vector space, we must have $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.

4. Let $z_1, z_2 \in \mathbb{C}$ and let $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Then for all $w \in \mathbb{C}$, we have

$$\begin{aligned} f_*(z_1\phi_1 + z_2\phi_2)(w) &= (f \circ (z_1\phi_1 + z_2\phi_2))(w) \\ &= f((z_1\phi_1 + z_2\phi_2)(w)) \\ &= f(z_1(\phi_1(w)) + z_2(\phi_2(w))) \\ &= z_1 f(\phi_1(w)) + z_2 f(\phi_2(w)) \\ &= z_1(f \circ \phi_1)(w) + z_2(f \circ \phi_2)(w) \\ &= z_1(f_*\phi_1)(w) + z_2(f_*\phi_2)(w) \\ &= (z_1(f_*\phi_1) + z_2(f_*\phi_2))(w). \end{aligned}$$

It follows that f_* is $\mathbb{C}$-linear.

5. Choose an eigenvector $v \in V$ for f corresponding to the eigenvalue $\lambda \in \mathbb{R}$. Let $\phi\colon \mathbb{C} \to V$ be the unique $\mathbb{R}$-linear map given by mapping $1 \mapsto v$ and $i \mapsto 0$ (note that $(1, i)$ is an ordered basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space and hence any $\mathbb{R}$-linear map out of $\mathbb{C}$ is completely determined by where it maps the ordered basis $(1, i)$). Then observe that for all $a + ib \in \mathbb{C}$, we have

$$\begin{aligned}
(f_*\phi)(a+ib) &= (f \circ \phi)(a+ib) \\
&= f(\phi(a+ib)) \\
&= f(a\phi(1) + b\phi(i)) \\
&= f(av) \\
&= af(v) \\
&= a\lambda v \\
&= \lambda av \\
&= \lambda(a\phi(1) + b\phi(i)) \\
&= \lambda\phi(a+ib).
\end{aligned}$$

It follows that $f_*\phi = \lambda\phi$. Thus λ is an eigenvalue for f_* with ϕ being a corresponding eigenvector.

1.1.3 Problem 3

Exercise 3. Let $f\colon V \to V$ be any linear map of vector spaces over a field K. Define an action of $K[X]$ on V as follows: for any polynomial $p(X)$

Solution 3.

We give V the structure of a $K[X]$-module by defining

$$p(X) \cdot v = p(f)(v) \tag{7}$$

for all $p(X) \in K[X]$ and for all $v \in V$. Let $v, w \in \ker(p(X))$ and let $a, b \in K$. Then

$$\begin{aligned}
p(X) \cdot (av + bw) &= p(f)(av + bw) \\
&= \sum_{i=0}^{n} c_i f^i(av + bw) \\
&= \sum_{i=0}^{n} c_i (af^i(v) + bf^i(w)) \\
&= a\sum_{i=0}^{n} c_i f^i(v) + b\sum_{i=0}^{n} c_i f^i(w) \\
&= a(p(X) \cdot v) + b(p(X) \cdot w) \\
&= 0 + 0 \\
&= 0.
\end{aligned}$$

Thus $av + bw \in \ker(p(X))$ which implies $\ker(p(X))$ is a linear subspace of V. In particular, when $p(X) = X - \lambda$ where $\lambda \in K$, we have

$$\begin{aligned}
v \in \ker(p(X)) &\iff v \in \ker(X - \lambda) \\
&\iff (X - \lambda) \cdot v = 0 \\
&\iff (f - \lambda)(v) = 0 \\
&\iff f(v) = \lambda v.
\end{aligned}$$

Thus $v \in \ker(p(X))$ if and only if v is an eigenvector of f with eigenvalue λ. Therefore $\ker(p(X)) = E_\lambda$ where E_λ is the eigenspace of f with respect to λ.

Now write

$$p(X) = \sum_{i=0}^{m} c_i X^i \quad \text{and} \quad q(X) = \sum_{j=0}^{n} d_j X^j$$

We first show that

$$\ker(p(X)q(X)) = \ker(p(X)) + \ker(q(X)). \tag{8}$$

Let $v \in \ker(p(X)) + \ker(q(X))$. Write $v = v_1 + v_2$ where $v_1 \in \ker(p(X))$ and $v_2 \in \ker(q(X))$. Then

$$\begin{aligned}
(p(X)q(X)) \cdot v &= p(X) \cdot (q(X) \cdot v) \\
&= p(X) \cdot (q(X) \cdot (v_1 + v_2)) \\
&= p(X) \cdot (q(X) \cdot v_1 + q(X) \cdot v_2) \\
&= p(X) \cdot (q(X) \cdot v_1) \\
&= (p(X)q(X)) \cdot v_1 \\
&= (q(X)p(X)) \cdot v_1 \\
&= q(X) \cdot (p(X) \cdot v_1) \\
&= q(X) \cdot 0 \\
&= 0
\end{aligned}$$

implies $v \in \ker(p(X)q(X))$. Thus $\ker(p(X)) + \ker(q(X)) \subseteq \ker(p(X)q(X))$. For the reverse inclusion, choose $a(X), b(X) \in K[X]$ so that

$$a(X)p(X) + b(X)q(X) = 1. \tag{9}$$

Let $v \in \ker(p(X)q(X))$. Using (9), write $v = v_1 + v_2$ where

$$v_1 = (b(X)q(X)) \cdot v \quad \text{and} \quad v_2 = (a(X)p(X)) \cdot v.$$

Then $v_2 \in \ker(q(X))$ since

$$\begin{aligned}
q(X) \cdot v_2 &= q(X) \cdot ((a(X)p(X)) \cdot v) \\
&= (q(X)a(X)p(X)) \cdot v \\
&= (a(X)p(X)q(X)) \cdot v \\
&= a(X) \cdot (p(X)q(X) \cdot v) \\
&= a(X) \cdot 0 \\
&= 0.
\end{aligned}$$

Similarly, $v_1 \in \ker(p(X))$ since

$$\begin{aligned}
p(X) \cdot v_1 &= p(X) \cdot ((b(X)q(X)) \cdot v) \\
&= (p(X)b(X)q(X)) \cdot v \\
&= (b(X)p(X)q(X)) \cdot v \\
&= b(X) \cdot (p(X)q(X) \cdot v) \\
&= b(X) \cdot 0 \\
&= 0.
\end{aligned}$$

Therefore $v \in \ker(p(X)) + \ker(q(X))$, and this implies $\ker(p(X)) + \ker(q(X)) \supseteq \ker(p(X)q(X))$.

To see that (8) is a direct sum, let $v \in \ker(p(X)) \cap \ker(q(X))$. Then

$$\begin{aligned}
v &= 1 \cdot v \\
&= (a(X)p(X) + b(X)q(X)) \cdot v \\
&= (a(X)p(X)) \cdot v + (b(X)q(X)) \cdot v \\
&= a(X) \cdot (p(X) \cdot v) + b(X) \cdot (q(X) \cdot v) \\
&= a(X) \cdot 0 + b(X) \cdot 0 \\
&= 0 + 0 \\
&= 0.
\end{aligned}$$

Thus $\ker(p(X)) \cap \ker(q(X)) = 0$ and so the sum (8) is direct.

We first prove by induction on $m \geq 2$ that for polynomials $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m$, we have

$$\ker(p_1(X)p_2(X) \cdots p_m(X)) = \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_m(X)). \tag{10}$$

The base case $m = 2$ was established in problem b.2. Now assume (10) is true for some $m \geq 2$. Let $p_i(X) \in K[X]$ such that $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m+1$. Since $\gcd(p_1(X), p_i(X)) = 1$ for all $2 \leq i \leq m+1$, we have $\gcd(p_1(X), p_2(X) \cdots p_{m+1}(X)) = 1$. Therefore

$$\begin{aligned}\ker(p_1(X)p_2(X)\cdots p_{m+1}(X)) &= \ker(p_1(X)) \oplus \ker(p_2(X)\cdots p_{m+1}(X)) \\ &= \ker(p_1(X)) \oplus \ker(p_2(X)) \oplus \cdots \oplus \ker(p_{m+1}(X)),\end{aligned}$$

where we used the base case on the first line and where we used the induction hypothesis to get from the first line to the second line.

To finish the problem, we just need to show that $V = \ker(c(X))$. Let $v \in V$. Then

$$\begin{aligned}c(X) \cdot v &= c(f)(v) \\ &= 0(v) \\ &= 0\end{aligned}$$

implies $v \in \ker(c(X))$. Therefore $V \subseteq \ker(c(X))$, which implies $V = \ker(c(X))$ (since $\ker(c(X))$ was already shown to be a subspace of V in problem b.1).

Let $E = \sum_{i=1}^{t} E_{\lambda_i}$ and let $c(X)$ be given by

$$c(X) = (X - \lambda_1) \cdots (X - \lambda_t),$$

where $\lambda_1, \ldots, \lambda_t$ are the distinct eigenvalues of f. Since $(X - \lambda_i)$ and $(X - \lambda_j)$ are relatively prime for all $1 \leq i < j \leq t$ and since $c(f) = 0$ on E, we can apply problem b.3 and obtain

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_t}$$

In particular $B_1 \cup B_2 \cup \cdots \cup B_t$ must be linearly independent: Suppose

$$\sum_{i=1}^{t} \sum_{j=1}^{m_i} a_{ij} u_{ij} = 0. \tag{11}$$

Then for each $1 \leq i \leq t$, we must have $\sum_{j=1}^{m_i} a_{ij} u_{ij} = 0$. Indeed, if $\sum_{j=1}^{m_k} a_{kj} u_{kj} \neq 0$ for some $1 \leq k \leq t$, then we can rearrange (11) to get

$$\sum_{j=1}^{m_k} a_{kj} u_{kj} = - \sum_{\substack{1 \leq i \leq t \\ i \neq k}} \sum_{j=1}^{m_i} a_{ij} u_{ij},$$

and so

$$\begin{aligned}0 \neq \sum_{j=1}^{m_k} a_{kj} u_{kj} &\\ &\in E_{\lambda_k} \cap \bigoplus_{\substack{1 \leq i \leq t \\ i \neq k}} E_{\lambda_i} \\ &= \{0\},\end{aligned}$$

gives us our desired contradiction. Thus, for each $1 \leq i \leq t$, we have

$$\sum_{j=1}^{m_i} a_{ij} u_{ij} = 0.$$

But this implies $a_{ij} = 0$ for all $1 \leq j \leq m_i$ since B_i is a basis for all $1 \leq i \leq t$. Thus $a_{ij} = 0$ for all $1 \leq i \leq t$ and $1 \leq j \leq m_i$, and hence $B_1 \cup B_2 \cup \cdots \cup B_t$ is linearly independent.

1.2 Abstract Algebra

1.2.1 Problem 1

Exercise 4. Let G be a group. If $x, y \in G$, we define the commutator of x and y to be $[x, y] = x^{-1}y^{-1}xy$ and denote the commutator subgroup by $[G, G]$. (recall that the commutator subgroup of G is the subgroup of G that is *generated* by the commutators of G).

1. Show that the inverse of a commutator is a commutator and that any conjugate of a commutator is a commutator.
2. Show that $[G, G]$ is a normal subgroup of G.
3. Show that if $\psi \in \mathrm{Aut}(G)$, then $\psi([G, G])$ is a subgroup of $[G, G]$.
4. Show that if $\varphi\colon G \to H$ is a homomorphism of groups, then $\operatorname{im}\varphi$ is abelian if and only if $[G, G]$ is a subgroup of $\ker\varphi$.
5. Show that if N is a subgroup of G which contains $[G, G]$, then N is a normal subgroup of G.

Solution 4. 1. Let $x, y \in G$. Then note that

$$\begin{aligned}[x, y]^{-1} &= (x^{-1}y^{-1}xy)^{-1} \\ &= y^{-1}x^{-1}yx \\ &= [y, x].\end{aligned}$$

2. First note that if $x, y, z \in G$, then we have

$$\begin{aligned}z[x, y]z^{-1} &= zx^{-1}y^{-1}xyz^{-1} \\ &= zx^{-1}z^{-1}zy^{-1}z^{-1}zxz^{-1}zyz^{-1} \\ &= [zxz^{-1}, zyz^{-1}].\end{aligned}$$

Therefore if $S = \{[x, y] \mid x, y \in G\}$, then $zSz^{-1} \subseteq S$ for all $z \in G$. This implies $z[G, G]z^{-1} \subseteq [G, G]$ for all $z \in G$. Thus $[G, G]$ is a normal subgroup of G.

3. We first note that $\psi([G, G])$ is a nonempty subset of $[G, G]$. Indeed, it is clearly nonempty since $e \in \psi([G, G])$. Also, for any $[x, y] \in [G, G]$, we have

$$\begin{aligned}\psi([x, y]) &= \psi(x^{-1}y^{-1}xy) \\ &= \psi(x)^{-1}\psi(y)^{-1}\psi(x)\psi(y) \\ &= [\psi(x), \psi(y)].\end{aligned}$$

Since $[G, G]$ is generated by all commutators, it follows that $\psi([G, G]) \subseteq [G, G]$. Finally note that if $H \leq G$, then $\psi(H) \leq G$. Indeed, $\psi(H)$ is nonempty since $e \in \psi(H)$, and if $\psi(x), \psi(y) \in \psi(H)$, then $\psi(x)\psi(y)^{-1} = \psi(xy^{-1}) \in \psi(H)$. In particular, $\psi([G, G]) \leq G$, and since $[G, G] \leq G$ and $\psi([G, G]) \subseteq [G, G]$, we see that $\psi([G, G]) \leq [G, G]$.

4. First suppose $\operatorname{im}\varphi$ is abelian. Then for any $x, y \in G$, we have

$$\begin{aligned}\varphi([x, y]) &= \varphi(x^{-1}y^{-1}xy) \\ &= \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) \\ &= \varphi(x)^{-1}\varphi(x)\varphi(y)^{-1}\varphi(y) \\ &= e,\end{aligned}$$

where we used the fact that $\operatorname{im}\varphi$ is abelian in order to get the third line from the second line. Thus all commutators belong to the kernel of φ, and since $[G, G]$ is generated by all commutators, it follows that $[G, G] \subseteq \ker\varphi$.

Conversely, suppose $[G,G] \subseteq \ker\varphi$. By the first isomorphism theorem, we have $\operatorname{im}\varphi \cong G/\ker\varphi$, so to show $\operatorname{im}\varphi$ is abelian, we just need to show that $G/\ker\varphi$ is abelian. Let $\overline{x},\overline{y} \in G/\ker\varphi$. Then observe that

$$\begin{aligned}\overline{xy} &= \overline{xy[y,x]} \\ &= \overline{xyy^{-1}x^{-1}yx} \\ &= \overline{yx}.\end{aligned}$$

It follows that $G/\ker\varphi$ is abelian.

5. Let $x \in G$ and let $y \in N$. Then note that $(xyx^{-1})y^{-1} = [x^{-1},y^{-1}] \in N$. It follows that $xyx^{-1} \in N$ since $y^{-1} \in N$. Thus N is a normal subgroup of G.

1.2.2 Problem 2

Exercise 5. Let R be a commutative ring with idenitty and let S be a nonempty subset of R. We say that S is **multiplicatively closed** if $s,t \in S$ implies $st \in S$. Additionally, we say that the set S is **saturated** if $st \in S$ implies $s,t \in S$.

1. Let $I \subseteq R$ be an ideal. Show that its complement $S := R\backslash I$ is saturated.
2. Let $I \subseteq R$ be an ideal. Show that its complement $S := R\backslash I$ is multiplicatively closed if and only if R/I is an integral domain.
3. Suppose that S is a multiplicatively closed subset of R that does not contain 0. Show that there is an ideal $\mathfrak{p}$ in R that is maximal with respect to the property that $\mathfrak{p} \cap S = \emptyset$.
4. Suppose that S is a multiplicatively closed subset of R that does not contain 0 and suppose that $\mathfrak{p}$ is maximal with respect to the property that $\mathfrak{p} \cap S = \emptyset$. Show that $\mathfrak{p}$ is necessarily prime.

Solution 5. 1. Suppose $s,t \in R$ and $st \in S$. Assume for a contradiction that $s \notin S$. Then $s \in I$, and since I is an ideal, this implies $st \in I$, which is a contradiction since $st \in S$. Therefore $s \in S$. A similar argument shows that $t \in S$.

2. Suppose S is multiplicatively closed. We will show that I is prime, which will imply R/I is an integral domain. Assume for a contradiction that I is not prime, so there exists $s,t \in R\backslash I$ such that $st \in I$. However this contradicts the fact that $S = R\backslash I$ is multiplicatively closed.

Conversely, suppose R/I is an integral domain, so I is a prime ideal. Assume for a contradiction that S is not multiplicatively closed. Then there exists $s,t \in S$ such that $st \notin S$. In other words, $s,t \notin I$ and $st \in I$. This contradicts the fact that I is a prime ideal.

(3 and 4). We appeal to Zorn's Lemma. We define a partial order $(\mathcal{F},\subseteq)$ as follows: the underlying set is given by

$$\mathcal{F} = \{I \subseteq R \mid I \text{ is an ideal and } I \cap S = \emptyset\}.$$

The partial order $\subseteq$ is set inclusion. Note that $\mathcal{F}$ is nonempty since $0 \in \mathcal{F}$. Let $(I_\lambda)_{\lambda\in\Lambda}$ be a totally ordered subset of $\mathcal{F}$. We claim that $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an upper bound for $(I_\lambda)_{\lambda\in\Lambda}$. To see this, first we will show that $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an ideal in R. First note that $\bigcup_{\lambda\in\Lambda} I_\lambda$ is nonempty since $0 \in \bigcup_{\lambda\in\Lambda} I_\lambda$. Next, let $a,b \in R$ and let $x,y \in \bigcup_{\lambda\in\Lambda} I_\lambda$. Then $x \in I_\lambda$ and $y \in I_\mu$ for some $\lambda,\mu \in \Lambda$. Without loss of generality, say $\lambda \leq \mu$, thus $x,y \in I_\mu$. Then since I_μ is an ideal, we have $ax + by \in I_\mu \subseteq \bigcup_{\lambda\in\Lambda} I_\lambda$. Thus $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an ideal as claimed. Now we need to show that $\bigcup_{\lambda\in\Lambda} I_\lambda$ has nonempty intersection with S. This is clear though since

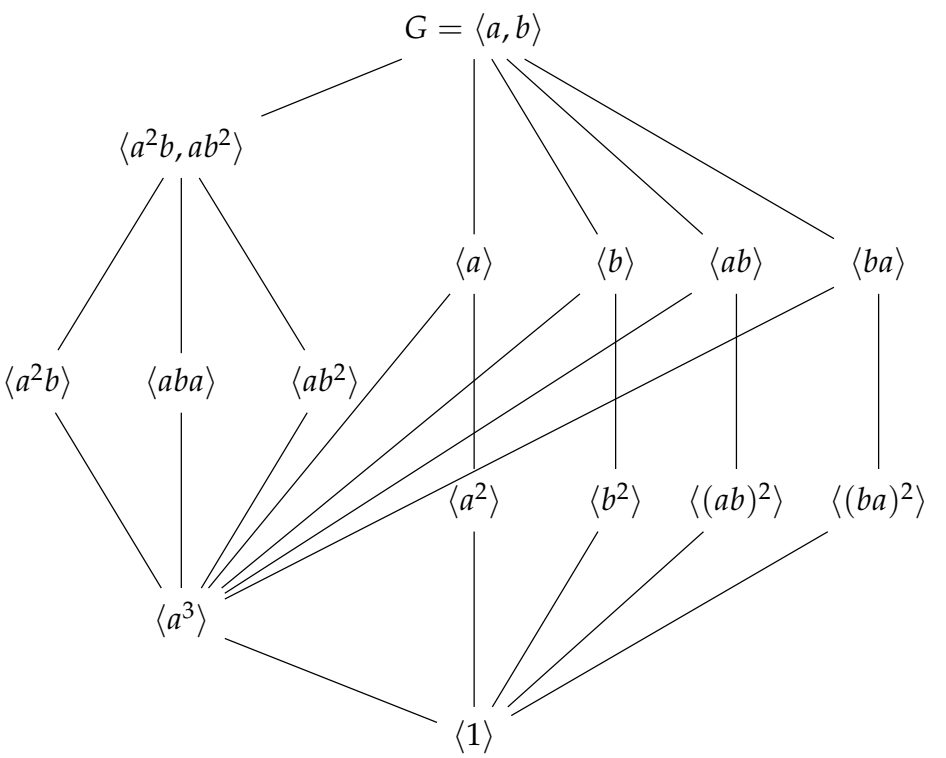
$$\begin{aligned}S \cap \left(\bigcup_{\lambda\in\Lambda} I_\lambda\right) &= \bigcup_{\lambda\in\Lambda} (S \cap I_\lambda) \\ &= \bigcup_{\lambda\in\Lambda} \emptyset \\ &= \emptyset.\end{aligned}$$

So we have shown that every totally ordered subset of $\mathcal{F}$ has an upper bound. We may therefore apply Zorn's Lemma to get an ideal $\mathfrak{p} \subseteq R$ which is maximal which respect to the property that $\mathfrak{p} \cap S = \emptyset$.

We now want to show now that $\mathfrak{p}$ is necessarily a prime ideal. Assume for a contradiction that $\mathfrak{p}$ is not a prime ideal. Then there exists $x, y \in R \backslash \mathfrak{p}$ such that $xy \in \mathfrak{p}$. Since S is multiplicatively closed, we cannot have both $x \in S$ and $y \in S$. Without loss of generality, say $x \notin S$. Then $\mathfrak{p} + \langle x \rangle$ is an ideal which has nonempty intersection with S (since $x \notin S$) and which strictly contains $\mathfrak{p}$. This contradicts maximality of $\mathfrak{p}$.

1.2.3 Problem 3

Exercise 6. In this problem G refers to the group of order 24 whose subgroup lattice appears below. You must fully justify each answer for full credit.



1. Show that in any group, a subgroup of order 2 is normal if and only if it is contained in the center.
2. Partition the fifteen subgroups into equivalence classes by conjugacy.
3. Is G solvable? Nilpotent?
4. What familiar group is the qoutient $G/\langle a^3 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.
5. What familiar group is the subgroup $\langle a^2b, ab^2 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.
6. What familiar group is the quotient $\langle a^2b, ab^2 \rangle / \langle a^3 \rangle$ isomorphic to? Use the isomorphism theorems to justify your answer.

Solution 6. 1. Let H be any group and let N be a subgroup of H of order 2. If N is contained in the center of H, then it is clear that N is normal in H. Indeed, let $h \in H$ and $n \in N$. Then

$$\begin{aligned} hnh^{-1} &= nhh^{-1} \\ &= n \\ &\in N. \end{aligned}$$

implies N is normal in H. Now suppose N is normal in H. Write $N = \{e, n\}$, where e is the identity, and let $h \in H$. If $hnh^{-1} = e$, then $hn = h$, which implies $n = e$, a contradiction. Thus we must have $hnh^{-1} = n$. This implies N is contained in the center of H.

2. The table below partitions the fifteen subgroups by conjugacy.

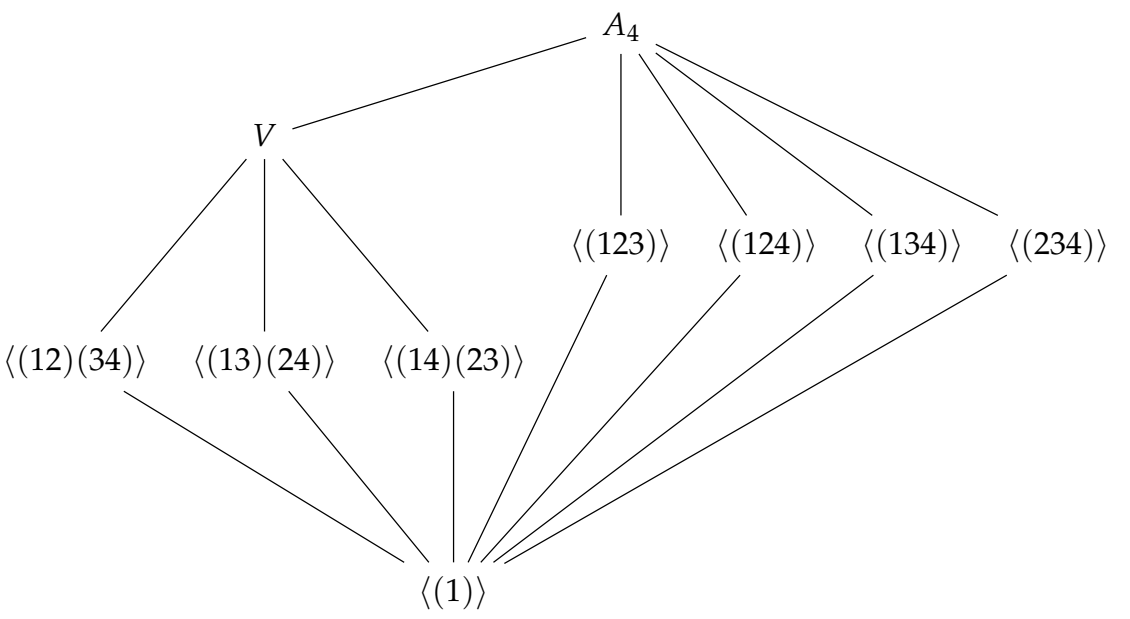
Equivalence Classes of Subgroups by Conjugacy
$\langle a \rangle$, $\langle b \rangle$, $\langle ab \rangle$, $\langle ba \rangle$
$\langle a^2 \rangle$, $\langle b^2 \rangle$, $\langle (ab)^2 \rangle$, $\langle (ba)^2 \rangle$
$\langle a^3 \rangle$
$\langle a^2 b \rangle$, $\langle aba \rangle$, $\langle ab^2 \rangle$
$\langle a^2 b, ab^2 \rangle$
$\langle a, b \rangle$

3. The group G is solvable. A composition series for G is given by

$$\langle 1 \rangle \triangleright \langle a^3 \rangle \triangleright \langle aba \rangle \triangleright \langle a^2 b, ab^2 \rangle \triangleright \langle a, b \rangle \tag{12}$$

with cyclic factors C_2, C_2, C_2, and C_3 respectively. On the other hand, G is *not* nilpotent. Indeed, if it were, then the quotient $G/\langle a^3 \rangle$ must be nilpotent as well. However, we shall see in the next part to this problem that $G/\langle a^3 \rangle \cong A_4$ which is not nilpotent.

4. The quotient group $G/\langle a^3 \rangle$ is isomorphic to A_4. The subgroup lattice of A_4 is given below.

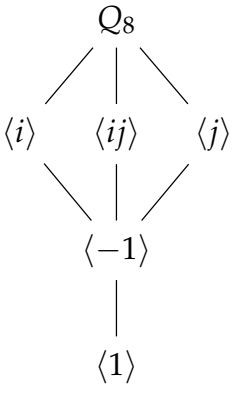


where $V = \langle (12)(34), (14)(23) \rangle$.

5. The group $\langle a^2 b, ab^2 \rangle$ is isomorphic to the quaternion group

$$Q_8 = \langle i, j \mid i^2 = -1, j^2 = -1, ij = -ij \rangle.$$

The subgroup lattice of Q_8 is given below



An isomorphism from $\langle a^2 b, ab^2 \rangle$ is given by $a^2 b \mapsto i$ and $ab^2 \mapsto j$.

6. The group $\langle a^2b, ab^2\rangle/\langle a^3\rangle$ is isomorphic to the Klein four-group K_4. Indeed, we obtain a group homomorphism $\langle a^2b, ab^2\rangle \to K_4$ by the composition

$$\langle a^2b, ab^2\rangle \xrightarrow{\cong} Q_8 \to Q_8/\langle -1\rangle \cong K_4.$$

The kernel of the group homomorphism $\langle a^2b, ab^2\rangle$ is $\langle a^3\rangle$. Thus by the first isomorphism theorem, we have

$$\langle a^2b, ab^2\rangle/\langle a^3\rangle \cong K_4.$$

2 Summer 2019

2.1 Linear Algebra

2.1.1 Problem 1

Exercise 7. Fix an integer $d \geq 2$ and consider the real vector space

$$V_d = \mathbb{R}[x]_{<d} = \{a_0 + a_1x + \cdots + a_{d-1}x^{d-1} \mid a_0, \ldots, a_{d-1} \in \mathbb{R}\}.$$

For all $f, g \in V_d$, define

$$\langle f, g\rangle = \int_0^1 fg\mathrm{d}x$$

where fg is the usual product of f and g from calculus.

1. Prove that $\langle \cdot, \cdot\rangle$ is an inner product on V_d.
2. In the case $d = 3$, apply Gram-Schmidt process to the ordered basis $(1, x, x^2)$ to find an orthonormal ordered basis for V_3. Then consider the subspace $W = \mathrm{span}_{\mathbb{R}}(1 - 2x)$ and find a basis for $W^{\perp}$.
3. Let $D\colon V_d \to V_d$ be the differentiation operator

$$D(f) = f' = \frac{\mathrm{d}f}{\mathrm{d}x},$$

   which is a linear transformation. Find the matrix representing D with respect to the order basis $(1, x, \ldots, x^{d-1})$. Prove or disprove: D is an isomorphism.
4. Prove or disprove: D is diagonalizable.
5. Compute $D^*(a_0 + a_1x + \cdots + a_{d-1}x^{d-1})$ where $D^*\colon V \to V$ is the adjoint of D.

Solution 7. 1. First we show linearity in the first argument when the second argument is fixed. In fact, this follows from linearity of multiplication and linearity of integration: let $a, b \in \mathbb{R}$ and $f, g, h \in V_d$, then

$$\begin{aligned}\langle af + bg, h\rangle &= \int_0^1 (af + bg)h\mathrm{d}x \\ &= \int_0^1 (afh + bgh)\mathrm{d}x \\ &= a\int_0^1 fh\mathrm{d}x + b\int_0^1 gh\mathrm{d}x \\ &= a\langle f, h\rangle + b\langle g, h\rangle.\end{aligned}$$

Next we show $\langle \cdot, \cdot\rangle$ is symmetric. This follows from commutativity of multiplication: let $f, g \in V_d$, then

$$\begin{aligned}\langle f, g\rangle &= \int_0^1 fg\mathrm{d}x \\ &= \int_0^1 gf\mathrm{d}x \\ &= \langle g, f\rangle.\end{aligned}$$

Finally, we show positive-definiteness of $\langle \cdot, \cdot \rangle$. This follows from the following fact about Lebesgue integration (or more generally integration over any measurable space): if f is any nonnegative Lebesgue measurable function, then $\int_0^1 f \mathrm{d}x = 0$ implies $f = 0$ almost everywhere. In particular, if $f \in V_d$, then

$$0 = \langle f, f \rangle = \int_0^1 f^2 \mathrm{d}x$$

implies $f^2 = 0$ almost everywhere, and since f^2 is just a polynomial, we in fact have $f^2 = 0$ everywhere, thus $f = 0$.

2. We first set $u_1 = 1$. Next we set

$$\begin{aligned} u_2 &= x - \frac{\langle x, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \\ &= x - \frac{\int_0^1 x \mathrm{d}x}{\int_0^1 \mathrm{d}x} \\ &= x - 1/2. \end{aligned}$$

Finally we set

$$\begin{aligned} u_3 &= x^2 - \frac{\langle x^2, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 - \frac{\langle x^2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \\ &= x^2 - \frac{\int_0^1 x^2 (x - 1/2) \mathrm{d}x}{\int_0^1 (x - 1/2)^2 \mathrm{d}x} (x - 1/2) - \frac{\int_0^1 x^2 \mathrm{d}x}{\int_0^1 \mathrm{d}x} \\ &= x^2 - 1(x - 1/2) - \frac{1}{3} \\ &= x^2 - x + 1/6. \end{aligned}$$

So (u_1, u_2, u_3) is an ordered orthogonal basis. To get an orthonormal basis, we set

$$\begin{aligned} v_1 &= \frac{u_1}{\|u_1\|} \\ &= \frac{1}{\sqrt{\int_0^1 \mathrm{d}x}} \\ &= 1. \end{aligned}$$

Next we set

$$\begin{aligned} v_2 &= \frac{u_2}{\|u_2\|} \\ &= \frac{x - 1/2}{\sqrt{\int_0^1 (x - 1/2)^2 \mathrm{d}x}} \\ &= \sqrt{12}(x - 1/2). \end{aligned}$$

Finally we set

$$\begin{aligned} v_3 &= \frac{u_3}{\|u_3\|} \\ &= \frac{x^2 - x + 1/6}{\sqrt{\int_0^1 (x^2 - x + 1/6)^2 \mathrm{d}x}} \\ &= \sqrt{180}(x^2 - x + 1/6). \end{aligned}$$

So (v_1, v_2, v_3) is an ordered orthonormal basis.

3. For each $0 \leq i \leq d-1$, we have

$$D(x^i) = ix^{i-1}.$$

Thus the matrix representation of D with respect to the ordered basis $\mathbf{x} = (1, x, \ldots, x^{d-1})$ is given by

$$[D]_{\mathbf{x}} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & d-1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

From this, it's easy to see that $\det D = 0$, which implies D is not an injective (and hence not an isomorphism).

4. The map D cannot be diagonalizable since the only eigenvectors for D are the constant polynomials. Indeed, if f is a nonconstant polynomial of degree i where $1 \leq i \leq d-1$, then $D(f)$ will have degree $i-1$, and thus f cannot be a constant multiple times $D(f)$. So D cannot have an eigenbasis, which means D cannot be diagonalizable.

Alternatively, if we let $\mathbf{x}' = (1, x, x^2/2, \ldots, x^{d-1}/(d-1))$. Then the matrix representation of D with respect to $\mathbf{x}'$ is given by

$$[D]_{\mathbf{x}'} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

This matrix respresentation also gives the Jordan canonical form of D. In particular D is not diagonalizable.

5. Using the fact that $[D^*]_{\mathbf{x}^*} = [D]_{\mathbf{x}}^\top$, we have

$$\begin{aligned} [D^*]_{\mathbf{x}^*} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} &= \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \ddots & \vdots \\ 0 & 2 & 0 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d-1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ a_0 \\ 2a_1 \\ \vdots \\ (d-1)a_{d-2} \end{pmatrix}. \end{aligned}$$

Therefore

$$D^*(a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}) = a_0 x + 2a_1 x^2 + \cdots + (d-1)a_{d-2}x^{d-1}.$$

2.1.2 Problem 2

Exercise 8. Let $p \in \mathbb{R}$ and let

$$A_p = \begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{pmatrix}.$$

1. Find the characteristic and the minimal polynomial of A_p.
2. Find the Jordan normal form J of A_p and a matrix S such that $A = SJS^{-1}$.

3. Prove that
$$V[A_p] = \{a_0 I + a_1 A_p + \cdots + a_n A_p^n \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}$$
with the usual matrix addition and scalar multiplication is a vector space over $\mathbb{R}$.

4. Find the dimension and a basis for $V[A_p]$.

Solution 8. 1. The characteristic polynomial of A_p is given by
$$\begin{aligned}\chi_{A_p}(T) &= \det \begin{pmatrix} T-4 & -1 & -p \\ 0 & T-5 & -1 \\ 0 & -1 & T-5 \end{pmatrix} \\ &= (T-4)((T-5)^2+1) \\ &= (T-4)^2(T-6).\end{aligned}$$
Since the minimal polynomial divides χ_{A_p} and shares the same roots as χ_{A_p}, we see that the minimal polynomial is either given by
$$\pi_{A_p}(T) = (T-4)(T-6) \quad \text{or} \quad \pi_{A_p}(T) = (T-4)^2(T-6).$$
Let us check for which values of $p \in \mathbb{R}$ do we have $\pi_{A_p}(T) = (T-4)(T-6) = T^2 - 10T + 24$. We calculate
$$\begin{aligned}\begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{pmatrix}^2 - 10 \begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{pmatrix} + 24 &= \begin{pmatrix} 16 & 9+p & 1+9p \\ 0 & 26 & 10 \\ 0 & 10 & 26 \end{pmatrix} - 10 \begin{pmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{pmatrix} + 24 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 16-40+24 & (9+p)-10 & (1+9p)-10p \\ 0 & 26-50+24 & 10-10 \\ 0 & 10-10 & 26-50+24 \end{pmatrix} \\ &= \begin{pmatrix} 0 & p-1 & 1-p \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.\end{aligned}$$
Thus we have
$$\pi_{A_p}(T) = \begin{cases} (T-4)(T-6) & \text{if } p = 1 \\ (T-4)^2(T-6) & \text{else} \end{cases}$$

2. First suppose $p = 1$. In this case, we have
$$\ker(A_1 - 6) = \mathbb{R} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{and} \quad \ker(A_1 - 4) = \mathbb{R} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}.$$
Thus
$$J_1 = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix} \quad \text{and} \quad S_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix}.$$
Now suppose $p \neq 1$. In this case, we have
$$\ker(A_p - 6) = \mathbb{R} \begin{pmatrix} 1+p \\ 2 \\ 2 \end{pmatrix}, \quad \ker(A_p - 4) = \mathbb{R} \begin{pmatrix} 1-p \\ 0 \\ 0 \end{pmatrix}, \quad \text{and} \quad \ker((A_p-4)^2) = \mathbb{R} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 1-p \\ 0 \\ 0 \end{pmatrix}.$$
Thus
$$J_p = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1+p & 1-p & 0 \\ 2 & 0 & 1 \\ 2 & 0 & -1 \end{pmatrix}.$$

3 and 4. Observe that
$$\mathbb{R}[X]/\langle \pi_{A_p}(X) \rangle \cong V[A_p]$$
via the map $\overline{X} \mapsto A_p$. In particular, $\dim V[A_p] = \deg(\pi_{A_p}(X))$. Thus if $p = 1$, then $\dim V[A_p] = 2$ and (I, A_p) is an ordered basis for $V[A_p]$. If $p \neq 1$, then $\dim V[A_p] = 3$ and (I, A_p, A_p^2) is an ordered basis for $V[A_p]$.

2.1.3 Problem 3

Solution 9. 2. Assume for a contradiction that x and y do not correspond to the same eigenvalue, say $Tx = \lambda x$ and $Ty = \mu y$ with $\lambda \neq \mu$. Then x and y are linearly independent: suppose $ax + by = 0$ for some $a, b \in K$. Then

$$\begin{aligned} 0 &= T(0) \\ &= T(ax + by) \\ &= \lambda ax + \mu by \\ &= -\lambda by + \mu by \\ &= (\mu - \lambda)by. \end{aligned}$$

Since $\mu \neq \lambda$, we must have $by = 0$, which implies $b = 0$. Thus $ax = 0$, which implies $a = 0$. This shows that x and y are linearly independent.

Now suppose that $T(x + y) = \gamma(x + y)$. Then

$$\begin{aligned} \lambda x + \mu y &= Tx + Ty \\ &= T(x + y) \\ &= \gamma(x + y) \\ &= \gamma x + \gamma y \end{aligned}$$

implies $\lambda = \gamma$ and $\mu = \gamma$ by linear independence of x and y. This is a contradiction. Thus x and y must correspond to the same eigenvalue.

3. Let v be an eigenvector of T corresponding to the eigenvalue λ. Then we have

$$\begin{aligned} \lambda\langle v, v\rangle &= \langle \lambda v, v\rangle \\ &= \langle Tv, v\rangle \\ &= \langle v, Tv\rangle && \text{(self adjointness of } T\text{)} \\ &= \langle v, \lambda v\rangle \\ &= \overline{\lambda}\langle v, v\rangle. \end{aligned}$$

Since $v \neq 0$ by definition of being an eigenvector, we must have $\langle v, v\rangle \neq 0$ by positive-definiteness of the inner-product. This implies $\lambda = \overline{\lambda}$, and hence λ is real.

4. Let A be a self-adjoint complex $n \times n$ matrix satisfying $A^3 = 2A + 4I$ and let $\pi_A(X)$ be the minimal polynomial of A over $\mathbb{C}$. Since $X^3 - 2X - 4$ kills A, we see that $\pi_A(X) \mid X^3 - 2X - 4$. Now observe that

$$X^3 - 2X - 4 = (X - 2)(X + 1 - i)(X + 1 + i).$$

The minimal polynomial of A over $\mathbb{C}$ cannot have complex roots, otherwise A would have complex eigenvalues (which contradicts the fact that A is self-adjoint). So we must have $\pi_A(X) \mid X - 2$, which implies $\pi_A(X) = X - 2$. In particular, A must have the form

$$A = UDU^{-1} = 2I$$

where U is a unitary matrix and where

$$D = \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 2 \end{pmatrix}$$

2.2 Abstract Algebra

2.2.1 Problem 1

Exercise 9. Let G be a finite group acting on itself by conjugation. In this problem, you may assume basic results, such as the orbit-stabilizer theorem, or classification of finite abelian groups, provided that you properly state them.

1. Characterize the orbits, stabilizers, kernels, and fixed points of this action. Your answer should be in terms of familiar group-theoretic objects, not just the definitions of these terms.
2. Prove that the size of any conjugacy class divides $|G|$.
3. Show that if G contains an element $x \in G$ that has exactly two conjugates, then G cannot be simple.
4. Prove that if G is a p-group, then its center is non-trivial.
5. Classify all simple p-groups, with proof. You may use the results of the previous parts, even if you could not prove them.

Solution 10. 1. First let us introduce some notation. Let $x \in G$. The orbit of x with respect to the conjugacy action is denoted $\mathrm{Orb}_G(x)$ and is given by

$$\mathrm{Orb}_G(x) = \{yxy^{-1} \mid y \in G\} = \mathrm{K}_x$$

where K_x is the conjugacy class of x. The stabilizer of x with respect to the conjugacy action is denoted $\mathrm{Stab}_G(x)$ and is given by

$$\begin{aligned}\mathrm{Stab}_G(x) &= \{y \in G \mid yxy^{-1} = x\} \\ &= \{y \in G \mid yx = xy\} \\ &= \mathrm{Z}(x),\end{aligned}$$

where $\mathrm{Z}(x)$ is the centralizer of x (the set of all elements in G which commute with x). Note that the conjugacy class of x has the same size as the index of its centralizer:

$$|\mathrm{K}_x| = [G : \mathrm{Z}(x)]. \tag{13}$$

Indeed, we obtain (13) by applying the orbit-stablizer theorem with respect to the conjugacy action. The kernel of the action is denoted $\mathrm{Ker}_G(G)$ and is given by

$$\begin{aligned}\mathrm{Ker}_G(G) &= \{x \in G \mid xyx^{-1} = y \text{ for all } y \in G\} \\ &= \{x \in G \mid xy = yx \text{ for all } y \in G\} \\ &= \mathrm{Z}(G)\end{aligned}$$

where $\mathrm{Z}(G)$ is the center of G (the set of all elements in G which commute with everything). The fixed points of the conjugacy action is denoted $\mathrm{Fix}_G(G)$ and is given by

$$\begin{aligned}\mathrm{Fix}_G(G) &= \{x \in G \mid yxy^{-1} = x \text{ for all } y \in G\} \\ &= \{x \in G \mid yx = xy \text{ for all } y \in G\} \\ &= \mathrm{Z}(G).\end{aligned}$$

2. Any conjugacy class in G has the form K_x for some $x \in G$. The identity (13) implies $|\mathrm{K}_x|$ divides $|G|$.

3. Suppose contains a conjugacy class which has exactly two elements, say K_x. Then $\mathrm{Z}(x)$ has index 2 in G. This implies $\mathrm{Z}(x)$ is normal in G. To see this, consider the more general situation where H is subgroup of G having index 2. We claim that group multiplication in G induces a group structure on G/H. Indeed, write $G/H = \{\overline{e}, \overline{x}\}$ where e is the identity in G and x is an element in G which represents the nontrivial coset (so $x \notin H$). We want to show that multiplication in G gives rise to the multiplication table in G/H given by

$\cdot$	$\overline{e}$	$\overline{x}$
$\overline{e}$	$\overline{e}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{e}$

showing that $G/H \cong \mathbb{Z}/2\mathbb{Z}$. Clearly we have $\overline{ex} = \overline{x} = \overline{xe}$ and $\overline{ee} = \overline{e}$. The only nontrivial multiplication that we need to show is $\overline{x}^2 = \overline{e}$. Assume for a contradiction that $\overline{x}^2 = \overline{x}$. Then $x = x^2y$ for some $y \in H$. This implies $e = xy$ which implies $x = y^{-1}$. However $x \notin H$ which is a contradiction (as H is closed under inverses). Thus

G/H inherits a group structure from multiplication in G, and the natural quotient map $\pi\colon G \to G/H$ has H as its kernel. It follows that H is normal.

4. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|Z(G)| = 1$. Let $x_1, \ldots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j}$ for each $1 \leq i < j \leq k$ and

$$G = \mathrm{Z}(G) \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{14}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ where for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (14) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction.

5. Suppose G is a simple p-group. By the previous problem, its center is nontrivial, in particular $\mathrm{Z}(G) \neq \{e\}$. Since the center of a group is always a normal subgroup and since G is simple, it follows that $G = \mathrm{Z}(G)$. Thus G is abelian. Any subgroup of an abelian group is a normal subgroup, so since G is simple abelian, it must contain no subgroups. Cauchy's Theorem tells us that there exists a subgroup of G whose order is p. This subgroup must be G itself. Thus $|G| = p$ which implies $G \cong C_p$ where C_p is the cyclic group of order p.

2.2.2 Problem 2

Exercise 10. The *First Isomorphism Theorem* holds for a variety of algebraic structures, and it relates the quotient of the domain of a homomorphism to its kernel and image.

1. Prove that the kernel of a group homomorphism is a subgroup and that it is normal.
2. State and prove the First Isomorphism Theorem for groups.
3. Prove that the kernel of a ring homomorphism is a two-sided ideal.
4. State and prove the First Isomorphism Theorem for rings.

Solution 11. (1 and 2). The first isomorphism theorem for groups is stated and proved as follows:

Theorem 2.1. *Let G and H be groups and let $\varphi\colon G \to H$ be a group homomorphism. Then*

1. *The kernel of φ is a normal subgroup of G.*
2. *The image of φ is a subgroup of H and moreover we have the isomorphism $G/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. 1. First let us check $\ker\varphi$ is a subgroup of G. It is nonempty since $\varphi(e) = e$ implies $e \in \ker\varphi$. Let $g_1, g_2 \in \ker\varphi$. Then observe that

$$\begin{aligned}\varphi(g_1 g_2^{-1}) &= \varphi(g_1)\varphi(g_2)^{-1} \\ &= ee \\ &= e\end{aligned}$$

implies $g_1 g_2^{-1} \in \ker\varphi$. It follows that $\ker\varphi$ is a subgroup of G.

Next, we check that $\ker\varphi$ is a normal subgroup of G. Let $g \in G$ and let $x \in \ker\varphi$. Then observe that

$$\begin{aligned}\varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g)^{-1} \\ &= \varphi(g)e\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= e\end{aligned}$$

implies $gxg^{-1} \in \ker \varphi$. It follows that $\ker \varphi$ is a normal subgroup of G.

2. First let us check $\operatorname{im} \varphi$ is a subgroup of H. It is nonempty since $\varphi(e) = e$ implies $e \in \operatorname{im} \varphi$. Let $\varphi(g_1), \varphi(g_2) \in \operatorname{im} \varphi$. Then observe that

$$\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1})$$

implies $\varphi(g_1)\varphi(g_2)^{-1} \in \operatorname{im} \varphi$. It follows that $\operatorname{im} \varphi$ is a subgroup of H.

Next, we define $\overline{\varphi}\colon G/\ker \varphi \to \operatorname{im} \varphi$ by

$$\overline{\varphi}(\overline{g}) = \varphi(g) \tag{15}$$

for all $\overline{g} \in G/\ker \varphi$. We need to check that (15) is well-defined. Let gx be another coset representative of $\overline{g}$ (so $\varphi(x) = e$). Then

$$\begin{aligned}
\overline{\varphi}(\overline{gx}) &= \varphi(gx) \\
&= \varphi(g)\varphi(x) \\
&= \varphi(g)e \\
&= \varphi(g) \\
&= \overline{\varphi}(\overline{g}).
\end{aligned}$$

Thus (15) is well-defined. Now we show $\overline{\varphi}$ gives us an isomorphism from $G/\ker \varphi$ to $\operatorname{im} \varphi$. It is a group homomorphism since if $g_1, g_2 \in G$, then

$$\begin{aligned}
\overline{\varphi}(\overline{g}_1\overline{g}_2) &= \varphi(g_1 g_2) \\
&= \varphi(g_1)\varphi(g_2) \\
&= \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).
\end{aligned}$$

It is also surjective since if $\varphi(g) \in \operatorname{im} \varphi$, then $\overline{\varphi}(\overline{g}) = \varphi(g)$. Finally, it is injective since

$$\begin{aligned}
&\overline{\varphi}(\overline{g}) = e \implies \varphi(g) = e \\
&\implies g \in \ker \varphi \\
&\implies \overline{g} = e.
\end{aligned}$$

Thus $\overline{\varphi}$ is in fact a group isomorphism. □

(3 and 4) The first isomorphism theorem for rings is stated and proved as follows:

Theorem 2.2. *Let R and S be rings and let $\varphi\colon R \to S$ be a ring homomorphism. Then*

1. *The kernel of φ is a two-sided ideal in R.*
2. *The image of φ is a subring of S and moreover we have the ring isomorphism $R/\ker \varphi \cong \operatorname{im} \varphi$.*

Proof. 1. First let us check $\ker \varphi$ is a two-sided ideal in R. First note that $\ker \varphi$ is an additive subgroup of R. Indeed, this follows from the first isomorphism theorem for groups. So to show that $\ker \varphi$ is a two-sided ideal in R, it suffices to show that it is closed under scalar multiplication: let $a \in R$ and let $x \in \ker \varphi$. Then

$$\begin{aligned}
\varphi(ax) &= a\varphi(x) \\
&= a \cdot 0 \\
&= 0
\end{aligned}$$

implies $ax \in \ker \varphi$. A similar computation shows that $xa \in \ker \varphi$. Thus $\ker \varphi$ is a two-sided ideal in R.

2. First let us check $\operatorname{im} \varphi$ is a subring of S. Again, it follows from the first isomorphism theorem for groups that $\operatorname{im} \varphi$ is an additive subgroup of S. So to show that $\operatorname{im} \varphi$ is a subring of R, it suffices to show that $\operatorname{im} \varphi$ is closed under multiplication in S and shares the same identity: let $\varphi(a), \varphi(b) \in \operatorname{im} \varphi$ where $a, b \in R$. Then since φ is a ring homomorphism, we have

$$\begin{aligned}
\varphi(a)\varphi(b) &= \varphi(ab) \\
&\in \operatorname{im} \varphi.
\end{aligned}$$

It follows that $\operatorname{im}\varphi$ is closed under multiplication in S. It also shares the same identity as S since ring homomorphisms by definition maps the multiplicative identity in R to the multiplicative identity in S.

Next, we define $\overline{\varphi}\colon R/\ker\varphi \to \operatorname{im}\varphi$ by

$$\overline{\varphi}(\overline{a}) = \varphi(a) \tag{16}$$

for all $\overline{a} \in R/\ker\varphi$. By the first isomorphism theorem for groups, $\overline{\varphi}$ is a well-defined group isomorphism. To see that $\overline{\varphi}$ is a *ring* isomorphism, it suffices to show that φ respects multiplication and that it maps the multiplicative identity in $R/\ker\varphi$ to the multiplicative identity in $\operatorname{im}\varphi$: let $\overline{a}, \overline{b} \in R/\ker\varphi$. Then

$$\begin{aligned}\overline{\varphi}(\overline{a}\overline{b}) &= \overline{\varphi}(\overline{ab}) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}).\end{aligned}$$

Also $\overline{\varphi}(\overline{1}) = \varphi(1) = 1$. It follows that $\overline{\varphi}$ gives a ring isomorphism from $R/\ker\varphi$ to $\operatorname{im}\varphi$. □

2.2.3 Problem 3

Exercise 11. Prove or disprove each of the following:

1. Every Euclidean domain is a principal ideal domain.
2. Every principal ideal domain is a Euclidean domain.
3. Every principal ideal domain is a unique factorization domain.
4. Every unique factorization domain is a principal ideal domain.
5. Every integral domain is a unique factorization domain.

Solution 12. 1. This is true. Let R be a Euclidean domain with respect to the Euclidean function $\mathrm{d}\colon R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ and let $I \subseteq R$ be an ideal. If $I = 0$, then we are done, so assume $I \neq 0$. Choose $x \in I\backslash\{0\}$ such that $\mathrm{d}(x)$ is minimal; that is, if $y \in I$, then $\mathrm{d}(x) \leq \mathrm{d}(y)$. We claim that $I = \langle x\rangle$. Indeed, let $y \in I$. Since R is a Euclidean domain, we have

$$y = qx + r \tag{17}$$

for some $q, r \in R$ where either $r = 0$ or $\mathrm{d}(r) < \mathrm{d}(x)$. Assume for a contradiction that $r \neq 0$, so $\mathrm{d}(r) < \mathrm{d}(x)$. Rewriting (17) as

$$r = y - qx$$

shows us that $r \in I$ since $x, y \in I$. However, this contradicts our choice of x with $\mathrm{d}(x)$ being minimal, since $r \in I$ and $\mathrm{d}(r) < \mathrm{d}(x)$. Therefore $r = 0$, which implies $y \in \langle x\rangle$. Thus $I \subseteq \langle x\rangle$, and since clearly $\langle x\rangle \subseteq I$, we in fact have $I = \langle x\rangle$. So every ideal in R is principal, which means R is a principal ideal domain.

2. This is false. For example, the ring $R = \mathbb{Z}\left[(1+\sqrt{-19})/2\right]$ is a principal ideal domain which is not a Euclidean domain. To see why it is not a Euclidean domain, first note that R is not a field since $\mathbb{Z} \subseteq R$ but $1/2 \notin R$. Therefore to prove R is not Euclidean, we will show that for no nonunit $a \in R$ is R/a represented by 0 and units. First we compute the norm of a typical element $\alpha = x + y(1+\sqrt{-19})/2$:

$$\mathrm{N}(\alpha) = x^2 + xy + 5y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4}. \tag{18}$$

This norm always takes values ≥ 0 (this is cleary from the second expression) and once $y \neq 0$ we have

$$\begin{aligned}\mathrm{N}(\alpha) &\geq \frac{19y^2}{4} \\ &\geq \frac{19}{4} \\ &> 4.\end{aligned}$$

In particular, the units are solutions to $N(\alpha) = 1$, which are ± 1:

$$R^\times = \{\pm 1\}.$$

The first few norm values are $0, 1, 4, 5, 7$, and 9. In particular, there is no element of R with norm 2 or 3. This and the fact that $R^\times \cup \{0|$ has size 3 are the key facts we will use.

If R were Euclidean, then there would be a nonunit a in R such that R/a is represented by 0 and units, so 0, 1, and -1. Perhaps $1 \equiv -1 \mod a$, but we definitely have $\pm 1 \not\equiv 0 \mod a$. Thus R/a has size 2 (if $1 \equiv -1 \mod a$) or size 3. We show this can't happen.

If R/a has size 2 then $2 \equiv 0 \mod a$, so $a \mid 2$ in R. Therefore $N(a) \mid 4$ in $\mathbb{Z}$. There are no elements of R with norm 2, so the only nonunits with norm dividing 4 are elements with norm 4. A check using (18) shows the only such numbers are ± 2. However, $R/\langle 2\rangle = R/\langle -2\rangle$ does not have size 2. For instance, 0, 1, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 2: the difference of two of these (different) numbers, divided by two, is never of the form $x + y(1+\sqrt{-19})/2$ for x and y in $\mathbb{Z}$.

Similarly, if $R/\langle a\rangle$ has size 3, then $a \mid 3$ in R, so $N(a) \mid 9$ in $\mathbb{Z}$. There is no element of R with norm 3, so a must have norm 9 (it doesn't have norm 1 since it is not a unit). The only elements of R with norm 9 are ± 3, so $a = \pm 3$. The ring $R/\langle 3\rangle - R/\langle -3\rangle$ does not have size 3: 0, 1, 2, and $(1+\sqrt{-19})/2$ are incongruent modulo ± 3. Since $R^\times \cup \{0\}$ has size 3 and R has no element a such that $R/\langle a\rangle$ has size 2 or 3, R can't be a Euclidean domain.

3. This is true. Let R be a principal ideal domain. Then R is a Noetherian, which means in particular that we can express any nonzero nonunit in R as a product of irreducibles. To see that such a factorization is unique, let a be a nonzero nonunit in R and let

$$p_1 p_2 \cdots p_r = a = q_1 q_2 \cdots q_s$$

be two factorizations of a into irreducibles. By relabeling terms if necessary, we may assume that $r \leq s$. We will prove by induction on $r \geq 1$ that (after reordering terms if necessary) $p_i \sim q_i$ for all $1 \leq i \leq r$, and $q_{r+1} \cdots q_s$ is a unit. In the base case, we have

$$p_1 = q_1 q_2 \cdots q_s.$$

Since R is a principal ideal domain, the irreducible element p_1 is in fact prime. Therefore $p_1 \mid q_j$ for some $1 \leq j \leq s$. Without loss of generality, say $p_1 \mid q_1$, so $q_1 = x_1 p_1$ for some $x_1 \in R$. Then we have

$$0 = p_1(1 - x_1 q_2 \cdots q_s).$$

Since R is a domain and $p_1 \neq 0$, this implies $1 = x_1 q_2 \cdots q_s$. Thus $q_2 \cdots q_s$ is a unit, and hence $p_1 \sim q_1$.

Now assume that $r > 1$ and that we have shown our claim to be true for all $1 \leq r' < r$. Again, p_1 is prime, and again we may assume without loss of generality that $q_1 = x_1 p_1$ for some $x_1 \in R$. Note that x_1 is necessarily a unit since q_1 is irreducible and since p_1 is a nonunit. So we have

$$0 = p_1(p_2 \cdots p_r - x_1 q_2 \cdots q_s).$$

Again, since R is a domain and $p_1 \neq 0$, this implies $p_2 \cdots p_r = x_1 q_2 \cdots q_s$. Now denote $q_2' = x_1 q_2$, so

$$p_2 \cdots p_r = q_2' \cdots q_s.$$

Now we can proceed by induction to conclude that $r = s$ and $p_i \sim q_i$ for all $1 \leq i \leq r$.

4. This is false. The ring $K[X, Y]$ provides a counterexample. Indeed, if R is a unique factorization domain, then $R[X]$ is a unique factorization domain. Let us state this in the form of a proposition and prove it:

Proposition 2.1. *Let R be a unique factorization domain. Then $R[T]$ is a unique factorization domain.*

Proof. Let $a(T)$ be a nonzero nonunit in $R[T]$ and let K be the fraction field of R. First note that $R[T]$ is Noetherian, and thus $a(T)$ has an irreducible factorization. Suppose

$$p_1(T) \cdots p_m(T) = a(T) = q_1(T) \cdots q_n(T)$$

are two irreducible factorizations of $a(T)$ in $R[T]$. By Gauss' Lemma, each $p_i(T)$ and $q_j(T)$ is irreducible in $K[T]$. Since $K[T]$ is a unique factorization domain, we see that $m = n$ and (perhaps after relabeling) $p_i(T) \sim q_i(T)$ in

$K[T]$. In particular, $p_i(T) = x_i q_i(T)$ for some $x_i \in K[T]^\times = K^\times$. Note that since $p_i(T), q_i(T) \in R[T]$, we must have $x_i \in R\backslash\{0\}$. Therefore

$$\begin{aligned} 0 &= p_1(T)\cdots p_m(T) - q_1(T)\cdots q_m(T) \\ &= p_1(T)\cdots p_m(T) - x_1\cdots x_m p_1(T)\cdots p_m(T) \\ &= p_1(T)\cdots p_m(T)(1 - x_1\cdots x_m) \\ &= a(T)(1 - x_1\cdots x_m), \end{aligned}$$

and since $a(T) \neq 0$ and $R[T]$ is a domain, this implies $1 = x_1\cdots x_n$, which implies each x_i is a unit in R. Thus $p_i(T) \sim q_i(T)$ in $R[T]$. □

5. This is false. The ring $\mathbb{Z}[\sqrt{-5}]$ provides a counterexample. In $\mathbb{Z}[\sqrt{-5}]$, we have two irreducible factorizations of 6. Namely

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{19}$$

Note that each factor in (19) is irreducible in $\mathbb{Z}[\sqrt{-5}]$. For instance, assume for a contradiction that $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ are nonunits in $\mathbb{Z}[\sqrt{-5}]$ such that

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \tag{20}$$

Taking norms on both sides of (20) gives us

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Since both $a + b\sqrt{-5}$ and $c + d\sqrt{-5}$ are nonunits in $\mathbb{Z}[\sqrt{-5}]$, we must have

$$a^2 + 5b^2 = 2 \quad \text{and} \quad c^2 + 5d^2 = 2.$$

However no such solution exists. Similar arguments shows that each factor in (19) must be irreducible in $\mathbb{Z}[\sqrt{-5}]$.

3 Winter 2019

3.1 Linear Algebra

3.1.1 Problem 1

Exercise 12. Let V be a finite-dimensional complex inner product space. A set of vectors $\{f_1, \ldots, f_m\}$ is called a **Parseval frame** for V if for every v, we have

$$v = \sum_{i=1}^{m} \langle v, f_i \rangle f_i.$$

1. Prove that every orthonormal basis of V is a Parseval frame.
2. Prove that there exists a Parseval frame which is not an orthonormal basis.
3. Prove that every linearly independent Parseval frame is an orthonormal basis.
4. Prove that $\{f_1, \ldots, f_m\}$ is a Parseval frame for V if and only if there is a complex inner product space W such that the following is true:
   (a) V is isometrically embedded in W, that is, there is an injective linear map $\phi\colon V \to W$ such that
   $$\langle v_1, v_2 \rangle_V = \langle \phi(v_1), \phi(v_2) \rangle_W$$
   for every $v_1, v_2 \in V$.
   (b) $\phi(f_i) = \mathrm{P}_{\phi(V)} e_i$ for some orthonormal basis $\{e_1, \ldots, e_m\}$ of W, where $\mathrm{P}_{\phi(V)}$ is the orthogonal projection onto the subspace $\phi(V)$.

Solution 13. 1. Let $\{v_1, \ldots, v_n\}$ be an orthonormal basis for V and let $v \in V$. Then we have

$$v = \sum_{i=1}^{n} a_i v_i \tag{21}$$

where $a_i \in \mathbb{C}$ are unique. Applying $\langle \cdot, v_i \rangle$ to both sides of (21) gives us $a_i = \langle v, v_i \rangle$. Thus $\{v_1, \ldots, v_n\}$ is a Parseval frame for V.

2. Consider the case where V is the vector space $\mathbb{C}^2$ with its standard Euclidean inner product. Set

$$\begin{aligned} v_1 &= \frac{\sqrt{3}}{2} e_1 - \frac{1}{2} e_2 \\ v_2 &= -\frac{\sqrt{3}}{2} e_1 - \frac{1}{2} e_2 \\ v_3 &= e_2. \end{aligned}$$

A quick calculation shows

$$\begin{aligned} \langle v, v_1 \rangle v_1 + \langle v, v_2 \rangle v_2 + \langle v, v_3 \rangle &= \frac{3}{2} \langle v, e_2 \rangle e_2 + \frac{3}{2} \langle v, e_1 \rangle e_1 \\ &= \frac{3}{2} \left(\langle v, e_2 \rangle e_2 + \langle v, e_1 \rangle e_1 \right) \\ &= \frac{3}{2} v. \end{aligned}$$

so $\{v_1, v_2, v_3\}$ almost does the trick. To get a Parseval frame, we just need to rescale: set $w_i = \sqrt{2/3} v_i$ for $i = 1, 2, 3$. Then

$$\begin{aligned} \langle v, w_1 \rangle w_1 + \langle v, w_2 \rangle w_2 + \langle v, w_3 \rangle w_3 &= \frac{2}{3} \left(\langle v, v_1 \rangle v_1 + \langle v, v_2 \rangle v_2 + \langle v, v_3 \rangle \right) \\ &= \frac{2}{3} \left(\frac{3}{2} v \right) \\ &= v. \end{aligned}$$

Thus $\{w_1, w_2, w_3\}$ is a Parseval frame.

3. Let $\{v_1, \ldots, v_m\}$ be a linearly independent Parseval frame for V. Then it is a basis for V. Indeed, if spans V since it is a Parseval frame for V: if $v \in V$, then

$$v = \sum_{i=1}^{m} \langle v, v_i \rangle v_i.$$

Also it is linearly independent by definition. Thus $\{v_1, \ldots, v_m\}$ is a basis for V. To see that it is an orthonormal basis, we must check that $\langle v_j, v_i \rangle = 0$ whenever $i \neq j$ and $\langle v_j, v_j \rangle = 1$. We have this because we can express v_j as

$$v_j = \sum_{i=1}^{m} \langle v_j, v_i \rangle v_i,$$

and by uniqueness of the coefficients, it follows that $\langle v_j, v_i \rangle = 0$ whenever $i \neq j$ and $\langle v_j, v_j \rangle = 1$.

4. To be lexicographically consistent, we will assume that V is an m-dimensional vector space and that $\{f_1, \ldots, f_n\}$ is a Parseval frame for V (so $m \leq n$). We may also identify V with $\mathbb{C}^m$ together with its standard Euclidean inner-product space. Let $\{e_1, \ldots, e_n\}$ be the standard

Consersely, suppose conditions (a) and (b) are true. Then for every $v \in V$, we have

$$\begin{aligned}
\phi\left(\sum_{i=1}^{m}\langle v, f_i\rangle f_i\right) &= \sum_{i=1}^{m}\langle v, f_i\rangle \phi(f_i) \\
&= \sum_{i=1}^{m}\langle \phi(v), \phi(f_i)\rangle \phi(f_i) \\
&= \sum_{i=1}^{m}\langle \phi(v), \phi(f_i)\rangle \mathrm{P}_{\phi(V)}(e_i) \\
&= \mathrm{P}_{\phi(V)}\left(\sum_{i=1}^{m}\langle \phi(v), \phi(f_i)\rangle e_i\right) \\
&= \\
&=
\end{aligned}$$

3.1.2 Problem 2

Exercise 13. Let V be a finite-dimensional vector space over $\mathbb{Q}$. Suppose that $A\colon V \to V$ is an invertible linear map such that $A^{-1} = \frac{1}{2}A^2 + A$.

1. Give all possibilities for the minimal and characteristic polynomials of A.
2. Prove that $\dim V$ is a multiple of 3.
3. Give an explicit example of how part (2) can fail if $\mathbb{Q}$ is replaced by $\mathbb{C}$.
4. Still assuming that V is a $\mathbb{C}$-vector space, prove that if $\dim V = 3$, then all such linear maps are similar.
5. Does part (4) still hold over $\mathbb{Q}$? Fully justify your answer.

Solution 14. 1. χ_A denote the characteristic polynomial of A and let π_A denote the minimal polynomial of A over $\mathbb{Q}$. Let

$$f(X) = X^3 + 2X^2 - 2.$$

From the definining equation of A, we see that $f(A) = 0$. It follows that $\pi_A \mid f$. In other words, we have

$$f = \pi_A g$$

for some $g \in \mathbb{Q}[X]$. Furthermore, f is irreducible over $\mathbb{Q}$ since it is irreducible over $\mathbb{Z}$ by Eisenstein's criterion at 2. Since both f and π_A are monic, this forces $g = 1$, so $f = \pi_A$. Finally, since χ_A and π_A share the same irreducible factors over $\mathbb{Q}$ and since π_A is irreducible over $\mathbb{Q}$, it follows that

$$\chi_A = \pi_A^n$$

for some $n \in \mathbb{N}$.

2. The dimension of V is equal to the degree of the characteristic polynomial of A, so

$$\begin{aligned}
\dim V &= \deg \chi_A \\
&= \deg(\pi_A^n) \\
&= n \deg \pi_A \\
&= 3n.
\end{aligned}$$

This implies $\dim V$ is a multiple of 3.

3. If $\mathbb{Q}$ is replaced by $\mathbb{C}$, then it may still have $\pi_A = f$, but it may no longer be the case that $\chi_A = \pi_A^n$ for some $n \in \mathbb{N}$. Indeed, over $\mathbb{C}$, the minimal polynomial factors, say as

$$\pi_A = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3),$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$ since $\pi'_A(X) = X(3X+4)$ has roots $X = 0$ and $X = -4/3$ (so $\pi'_A(\alpha_i) \neq 0$ for any $i = 1, 2, 3$). Then it is possible that the characteristic polynomial of A has the form

$$\chi_A = (X - \alpha_1)^2(X - \alpha_2)(X - \alpha_3).$$

Both χ_A and π_A share the same irreducible factors over $\mathbb{C}$, so there is no contradiction here. The Jordan canonical form for A in this case is given by the matrix

$$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_1 & 0 & 0 \\ 0 & 0 & \alpha_2 & 0 \\ 0 & 0 & 0 & \alpha_3 \end{pmatrix}.$$

So in this case, we see that $\dim V = 4$, which is not a multiple of 3.

4. I don't think we are given enough information here to conclude that all such linear maps are similar. Indeed, the minimal polynomial of A simply needs to divide f. Thus we could have $\pi_A = (X - \alpha_1)$ and $\chi_A = (X - \alpha_1)^3$. In this case, the Jordan canonical form for A is

$$\begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_1 & 0 \\ 0 & 0 & \alpha_1 \end{pmatrix}.$$

It is easy to check that this matrix satisfies f. If we make the further assumption that $\pi_A = f$, then since $\deg \chi_A = \dim V = \deg \pi_A$, and $\pi_A \mid \chi_A$, and π_A and χ_A both being monic forces $\pi_A = f$. In this case, the Jordan canonical form for A is

$$\begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}.$$

5. By part 1, we necessarily have $f = \pi_A$. Also $\dim V = 3$ implies $\pi_A = \chi_A$ by the same reasoning as in part 4. So the rational canonical form of A is

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

3.2 Abstract Algebra

3.2.1 Problem 1

Exercise 14. Let G be an additive abelian group. For each positive integer n, set

$$\Gamma_n(G) = \{g \in G \mid n^m g = 0 \text{ for some positive integer } m\}.$$

Let $\alpha\colon G \to H$ and $\beta\colon H \to K$ be homomorphisms of additive abelian groups.

1. Prove that $\Gamma_n(G)$ is a subgroup of G.
2. Prove that $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$ and that $\Gamma_n(\alpha)\colon \Gamma_n(G) \to \Gamma_n(H)$ defined by

   $$\Gamma_n(\alpha)(g) = \alpha(g)$$

   for all $g \in \Gamma_n(G)$ is a well-defined group homomorphism.
3. Prove that if α is injective, then so is $\Gamma_n(\alpha)$.
4. Prove or disprove that if α is surjective, then so is $\Gamma_n(\alpha)$.
5. Prove that if G is finitely generated, then $\Gamma_n(G)$ is finite.

Solution 15. 1. First note that $\Gamma_n(G)$ is nonempty since $0 \in \Gamma_n(G)$. Now let $g_1, g_2 \in \Gamma_n(G)$ and choose $m_1, m_2 \in \mathbb{Z}$ such that $n^{m_1} g_1 = n^{m_2} g_2 = 0$. Then

$$\begin{aligned} n^{m_1+m_2}(g_1 - g_2) &= n^{m_1+m_2} g_1 - n^{m_1+m_2} g_2 \\ &= n^{m_2}(n^{m_1} g_1) - n^{m_1}(n^{m_2} g_2) \\ &= n^{m_2} \cdot 0 - n^{m_1} \cdot 0 \\ &= 0. \end{aligned}$$

implies $g_1 - g_2 \in \Gamma_n(G)$. It follows that $\Gamma_n(G)$ is a subgroup of G.

2. Let $g \in \Gamma_n(G)$ and choose $m \in \mathbb{Z}$ such that $n^m g = 0$. Then

$$\begin{aligned} n^m \alpha(g) &= \alpha(n^m g) \\ &= \alpha(0) \\ &= 0. \end{aligned}$$

implies $\alpha(g) \in \Gamma_n(H)$. It follows that $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$.

Next we show that $\Gamma_n(\alpha)$ is a well-defined group homomorphism. First note that $\Gamma_n(\alpha)$ lands in $\Gamma_n(H)$ by what we've just shown. It is also a well-defined group homomorphism since it is just the restriction of $\alpha \colon G \to H$ to $\Gamma_n(G)$.

3. This follows from the fact that the restriction of an injective map is injective.

4. This is false. Consider the case where $G = \mathbb{Z}$, $H = \mathbb{Z}/2\mathbb{Z}$, and $n = 2$. Here, we have $\Gamma_2(\mathbb{Z}) = 0$ and $\Gamma_2(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Then the natural quotient map $\pi \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is surjective, but the induced map $\Gamma_n(\pi) \colon 0 \to \mathbb{Z}/2\mathbb{Z}$ clearly cannot be surjective.

5. First note that if G_1 and G_2 are two abelian groups, then we have

$$\Gamma_n(G_1 \oplus G_2) = \Gamma_n(G_1) \oplus \Gamma_n(G_2).$$

Indeed, if $(g_1, g_2) \in \Gamma_n(G_1 \oplus G_2)$, then we choose $m \in \mathbb{Z}$ such that $n^m(g_1, g_2) = 0$. This implies $n^m g_1 = 0$ and $n^m g_2 = 0$ which implies $g_1 \in \Gamma_n(G_1)$ and $g_2 \in \Gamma_n(G_2)$. Conversely, if $g_1 \in \Gamma_n(G_1)$ and $g_2 \in \Gamma_n(G_2)$, then we choose $m_1, m_2 \in \mathbb{Z}$ such that $n^{m_1} g_1 = 0$ and $n^{m_2} g_2 = 0$. This implies

$$\begin{aligned} n^{m_1+m_2}(g_1, g_2) &= (n^{m_2}(n^{m_1} g_1), n^{m_1}(n^{m_2} g_2)) \\ &= (0, 0) \end{aligned}$$

which implies $(g_1, g_2) \in \Gamma_n(G_1 \oplus G_2)$.

Now we can prove 5 easily as follows: by the fundamental theorem of finitely generated abelian groups, G is isomorphic to

$$\mathbb{Z}^r \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_s}$$

where $q_1, \ldots, q_s$ are powers of (not necessarily distinct) prime numbers and $r \in \mathbb{Z}_{\geq 0}$. It follows that

$$\begin{aligned} \Gamma_n(G) &\cong \Gamma_n(\mathbb{Z}^r \oplus \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_s}) \\ &= \Gamma_n(\mathbb{Z}^r) \oplus \Gamma_n(\mathbb{Z}_{q_1}) \oplus \cdots \oplus \Gamma_n(\mathbb{Z}_{q_s}) \\ &= 0 \oplus \Gamma_n(\mathbb{Z}_{q_1}) \oplus \cdots \oplus \Gamma_n(\mathbb{Z}_{q_s}). \end{aligned}$$

In particular, we see that $|\Gamma_n(G)| \leq q_1 \cdots q_s$.

4 Winter 2018

4.1 Problem 1

Exercise 15. Consider the matrix

$$A = \begin{pmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

where $a, b, c > 0$. Let λ_1, λ_2, and λ_3 denote the eigenvalues of A and suppose that $\lambda_1 \leq \lambda_2 \leq \lambda_3$.

1. Prove that $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$.
2. Prove that $\lambda_1, \lambda_2 < 0$ and $\lambda_3 > 0$.
3. Prove that if $v \in \mathbb{R}^3$, then $\langle Av, v\rangle \lambda_3 \leq \langle Av, Av\rangle$.
4. Show that
$$\lambda_3 \leq \frac{(a+b)^2 + (b+c)^2 + (a+c)^2}{2(a+b+c)}.$$

Solution 16. 1. Let λ be an eigenvalue of A and let $\mathbf{v}$ be a corresponding eigenvector. Then we have

$$\begin{aligned}
\lambda \mathbf{v}^\top \mathbf{v} &= (\lambda \mathbf{v})^\top \mathbf{v} \\
&= (A\mathbf{v})^\top \mathbf{v} \\
&= \mathbf{v}^\top A^\top \mathbf{v} \\
&= \mathbf{v}^\top A \mathbf{v} \\
&= \mathbf{v}^\top \lambda \mathbf{v} \\
&= \lambda \mathbf{v}^\top \mathbf{v}
\end{aligned}$$

Any eigenvector v of a symmetric matrix B mustObserve that if v is an eigenvector of

Here, we can appeal to the fact that A is a compact self-adjoint operator with respect to the Euclidean inner-product. Such an operator always has real eigenvalues. However let's prove that $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ in another way. A quick calculation using the Leibniz formula for computing determinants shows that the characteristic polynomial of A is given by

$$(X - \lambda_1)(X - \lambda_2)(X - \lambda_3) = \chi_A(X) = X^3 - (a^2 + b^2 + c^2)X - 2abc. \tag{22}$$

Expanding the product on the left side in (22) and equation coefficients gives us the relations

$$\begin{aligned}
\lambda_1 \lambda_2 \lambda_3 &= 2abc \\
\lambda_1 \lambda_2 + \lambda_1 \lambda_3 + \lambda_2 \lambda_3 &= -(a^2 + b^2 + c^2) \\
\lambda_1 + \lambda_2 + \lambda_3 &= 0.
\end{aligned}$$

Since $\lambda_1 \lambda_2 \lambda_3 = 2abc$ and $a, b, c > 0$ we must have $\lambda_3 > 0$ and either $\lambda_1, \lambda_2 < 0$ or $\lambda_1, \lambda_2 > 0$. Since $\lambda_1 + \lambda_2 + \lambda_3 = 0$ and $\lambda_3 > 0$, we must have $\lambda_1, \lambda_2 < 0$.

4.2 Problem 2

Exercise 16. Let V be a real finite-dimensional inner-product space with proper subspaces U and W. Let P_U and P_V be the orthogonal projections onto U and W respectively.

1. For this part of the problem suppose that $V = \mathbb{R}^n$ and $U = \operatorname{span}(u)$ for some vector $u \neq 0$. Prove that the matrix of P_U with respect to the standard basis of V is $uu^\top / (u^\top u)$.
2. Prove that $\operatorname{trace}(\mathrm{P}_U) = \dim U$.
3. Prove that $\ker(\mathrm{P}_W \mathrm{P}_U) = U^\perp \oplus (W^\perp \cap U)$

Solution 17. 1. Let $\mathbf{e} = (e_1, \ldots, e_n)$ denote the standard ordered basis of $\mathbb{R}^n$. Express u in terms of the ordered basis $\mathbf{e}$, say

$$u = \sum_{i=1}^{n} a_i e_i.$$

For each $1 \leq i \leq n$, we have

$$\begin{aligned}
\mathrm{P}_U(e_i) &= \frac{\langle e_i, u\rangle}{\langle u, u\rangle} u \\
&= \frac{1}{u^\top u} \sum_{j=1}^{n} a_i a_j e_j
\end{aligned}$$

Thus the entry in the (i,j) component of the matrix representation of P_U with respect to $\mathbf{e}$ is $a_i a_j/(u^\top u)$. This is also the same entry in the (i,j) component of the matrix $uu^\top/(u^\top u)$. Since the matrix representation of P_U with respect to $\mathbf{e}$ and the matrix $uu^\top/(u^\top u)$ are $n \times n$ matrices with the same entries, it follows that they must be equal.

2. Let $\mathbf{u} = (u_1, \ldots, u_m)$ be an ordered basis for U and let $\mathbf{u}' = (u'_1, \ldots, u'_{m'})$ be an ordered basis for $U^\perp$. Since $V = U \oplus U^\perp$ (we have this decomposition over any inner-product space), we see that $\mathbf{u} \cup \mathbf{u}'$ is an ordered basis for V. Since

$$\mathrm{P}_U(u_i) = u_i \quad \text{and} \quad \mathrm{P}_U(u'_{i'}) = 0$$

for all $1 \leq i \leq m$ and $1 \leq i' \leq m'$, we see that the matrix representation of P_U with respect to $\mathbf{u} \cup \mathbf{u}'$ is given by

$$[\mathrm{P}_U] = \begin{pmatrix} \mathrm{I}_m & 0 \\ 0 & 0 \end{pmatrix}$$

where I_m is the $m \times m$ identity matrix. Clearly we have

$$\operatorname{trace}(\mathrm{P}_U) = m = \dim U.$$

3. Let $v \in \ker(\mathrm{P}_W \mathrm{P}_U)$. Express v in terms of its decomposition in $U^\perp \oplus U$ as

$$v = v - \mathrm{P}_U(v) + \mathrm{P}_U(v),$$

where $v - \mathrm{P}_U(v) \in U^\perp$ and $\mathrm{P}_U(v) \in U$. To show that $v \in U^\perp \oplus (W^\perp \cap U)$, we just need to show that $\mathrm{P}_U(v) \in W^\perp \cap U$ or, more simply, $\mathrm{P}_U(v) \in W^\perp$ (as we already have since $\mathrm{P}_U(v) \in U$). This is clear though since

$$\mathrm{P}_W(\mathrm{P}_U(v)) = 0$$

implies $\mathrm{P}_U(v) \in \ker \mathrm{P}_W = W^\perp$.

Conversely, let $u + v \in U^\perp \oplus (W^\perp \cap U)$, so $u \in U^\perp$ and $v \in W^\perp \cap U$. Then

$$\begin{aligned} \mathrm{P}_W \mathrm{P}_U(u+v) &= \mathrm{P}_W(\mathrm{P}_U(v)) \\ &= \mathrm{P}_W(v) \\ &= 0 \end{aligned}$$

implies $u + v \in \ker \mathrm{P}_W \mathrm{P}_U$.

4.3 Problem 3

Exercise 17. Let S be an integral domain and let R be a subring of S such that $1_S \in R$. Let $s \in S$ be given, and let $R[s]$ denote the intersection of the subrings of S containing R and s.

1. Prove that the set $R[s]$ is the smallest subring of S containing R and s and that $R[s]$ is an integral domain.
2. Prove that
$$R[s] = \{f(s) \in S \mid f(X) \in R[X]\},$$
that is, $R[s]$ is the set of all elements $t \in S$ such that there is a polynomial $f(X) \in R[X]$ such that $t = f(X)$.
3. Prove that there exists a surjective ring homomorphism $\varphi\colon R[X] \to R[s]$ such that $\varphi(r) = r$ for all $r \in R$.
4. Prove that $\ker \varphi$ is a prime ideal of $R[X]$.
5. Prove or give a counterexample to the following statement: $\ker \varphi$ is a maximal ideal of $R[X]$.

Solution 18. 1. We first show that $R[s]$ is a subring of S. First note that $R[s]$ shares the identity in S. Indeed, if A is any subring of S which contains R and s, then $1_S \in A$ (by definition of what it means to be a subring). As A is arbitrary, this implies $1_S \in R[s]$. Now let $a, b \in R[s]$ and let A be a subring of S which contains R and s. Then $a, b \in A$, and since A is a ring, we have $a + b \in A$ and $ab \in A$. Since A is arbitrary, this implies $a + b \in R[s]$ and $ab \in R[s]$. It follows that $R[s]$ is a subring of S which contains R and s.

It is also clearly the *smallest* subring of S which contains R and s. Indeed, $R[s]$ is, by definition, the intersection of all subrings of S which contain R and s. Thus if A is a subring of S which contains R and s, then $R[s] \subseteq A$. Finally, note that $R[s]$ is an integral domain since it inherits this property from S. Indeed, if $a, b \in R[s]$ such that $ab = 0$, then since $a, b \in S$, we see that either $a = 0$ or $b = 0$.

(2 and 3). First we solve part 3. Let $\varphi\colon R[X] \to R[s]$ be the unique R-algebra homorphism a ring homomorphism such that $\varphi(X) = s$. Thus if $f(X) \in R[x]$, then $\varphi(f) = f(s)$. Clearly we have $\varphi(r) = r$ for all $r \in R$. Let us check that this is in fact a ring homomorphism. Let $f(X), g(X) \in R[X]$, say

$$f(X) = \sum_{i=0}^{\infty} a_i X^i \quad \text{and} \quad g(X) = \sum_{j=0}^{\infty} b_j X^j$$

where $a_i, b_j \in R$ and where $a_i, b_j = 0$ for all but finitely many i, j. Then

$$\begin{aligned}
\varphi(fg) &= \varphi\left(\sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k\right) \\
&= \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) s^k \\
&= \left(\sum_{i=0}^{\infty} a_i s^i\right)\left(\sum_{j=0}^{\infty} b_j s^j\right) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

Similarly

$$\begin{aligned}
\varphi(f+g) &= \varphi\left(\sum_{k=0}^{\infty}(a_k + b_k) X^k\right) \\
&= \sum_{k=0}^{\infty}(a_k + b_k) s^k \\
&= \sum_{k=0}^{\infty} a_k s^k + \sum_{k=0}^{\infty} b_k s^k \\
&= \varphi(f) + \varphi(g).
\end{aligned}$$

Thus φ is a ring homomorphism. We want to show that φ is surjective. Clearly we have

$$\operatorname{im}\varphi = \{f(s) \in S \mid f(X) \in R[X]\},$$

thus we are trying to show $\operatorname{im}\varphi = R[s]$. Note that $\operatorname{im}\varphi$ is a subring of S by the first isomorphism theorem for rings. Furthermore, $\operatorname{im}\varphi$ contains R and s. It follows that $R[s] \subseteq \operatorname{im}\varphi$. For the reverse inclusion, let A be any subring of S which contains R and s. Let $f(X)$ be any polynomial in $R[x]$, say

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

where $a_i \in R$ for all $0 \leq i \leq n$. Then since A is a ring which contains R and s, we must have

$$f(s) = \sum_{i=0}^{n} a_i s^i \in A.$$

In particular, $\operatorname{im}\varphi \subseteq A$. It follows that $\operatorname{im}\varphi \subseteq R[s]$.

4. Combining the first isomorphism theorem for rings with the fact that $\operatorname{im}\varphi = R[s]$, we see that

$$R[s] \cong R[X]/\ker\varphi.$$

Now since $R[s]$ is an integral domain, it follows that $\ker\varphi$ is a prime ideal in $R[X]$.

5. Clearly $\ker\varphi$ need not be a maximal ideal. Indeed, $\ker\varphi$ being a maximal ideal is equivalent to $\operatorname{im}\varphi$ being a field, however this may not happen. For instance, consider the case where $S, R = \mathbb{Z}$ and $s = 1$. Then $\operatorname{im}\varphi = \mathbb{Z}$ is not a field. Thus $\ker\varphi$ is not a maximal ideal.

4.4 Problem 4

Exercise 18. 1. Show that all groups of order 100 are semi-direct products of their Sylow p-subgroups. You may of course appeal to the Sylow theorems.

2. Explicitly classify the groups of order 100 which have cyclic Sylow p-subgroups as follows. Give a presentation (generators and fundamental relations) of a group from each isomorphism class and argue that your list is complete. Be sure to state any theorems to which you appeal.

3. Give an example of a group of order 100 which has at least one non-cyclic Sylow p-subgroup. Again, give the presentation for your example, and argue that it really does have order 100 and that it has a non-cyclic Sylow p-Subgroup.

Solution 19. 1. Let G be a group of order $100 = 2^2 \cdot 5^2$. Denote n_2 and n_5 to be the number of 2-Sylow subgroups of G and 5-Sylow subgroups of G respectively. The Sylow Theorems tells us that

$$n_5 \equiv 1 \bmod 5 \quad \text{and} \quad n_5 \mid 4.$$

The only possibility here is that $n_5 = 1$. Let P be a 2-Sylow subgroup of G and let Q be the 5-Sylow subgroup. Since $n_5 = 1$, it follows that Q is a normal subgroup of G (conjugating Q results in another 5-Sylow subgroup, which must be Q itself). It follows from the Second Isomorphism Theorem that PQ is a subgroup of G.

We claim that $|PQ| = |G|$ (which forces $PQ = G$). First note that since PQ is a subgroup of G, Lagranges Theorem tells us that $|PQ| \mid |G|$. Similarly since P and Q are both subgroups of PQ, we must have $4 \mid |PQ|$ and $25 \mid |PQ|$. This implies $100 \mid |PQ|$, that is, $|G| \mid |PQ|$. It follows that $|G| = |PQ|$ which implies $G = PQ$.

Finally, note that $P \cap Q = \{e\}$ since $|P|$ and $|Q|$ are relatively prime. Indeed, if $x \in P \cap Q$, then $\operatorname{ord} x$ must divide $\gcd(|P|, |Q|) = 1$. Thus $\operatorname{ord} x = 1$ which implies $x = e$. Therefore G is a semi-direct product of its Sylow p-subgroups.

2. Suppose that G has cyclic Sylow p-subgroups. Again let P be a Sylow 2-subgroup of G and let Q by the Sylow 5-subgroup of G. Suppose $P = \langle x \rangle$ and $Q = \langle y \rangle$. By part 1, G is a semidirect product of P and Q, thus every element in G can be expressed uniquely as $x^i y^j$ where $i \in \mathbb{Z}/4\mathbb{Z}$ and $j \in \mathbb{Z}/25\mathbb{Z}$. Furthermore, if $x^i y^j$ and $x^{i'} y^{j'}$ are two elements in G, then their product is

$$\begin{aligned}
(x^i y^j)(x^{i'} y^{j'}) &= x^i y^j x^{i'} y^{j'} \\
&= x^i (x^{i'} x^{-i'}) y^j x^{i'} y^{j'} \\
&= x^i x^{i'} (x^{-i'} y^j x^{i'}) y^{j'} \\
&= x^i x^{i'} (x^{-i'} y x^{i'})^j y^{j'} \\
&= x^i x^{i'} (y^{k^{i'}})^j y^{j'} \\
&= x^{i+i'} y^{jk^{i'}+j'}
\end{aligned}$$

where $x^{-1} y x = y^k$ where $k \in \mathbb{Z}/25\mathbb{Z}$. To see why the second to the last line holds, observe that

$$\begin{aligned}
x^{-2} y x^2 &= x^{-1}(x^{-1} y x) x \\
&= x^{-1} y^k x \\
&= (x^{-1} y x)^k \\
&= (y^k)^k \\
&= y^{k^2}.
\end{aligned}$$

More generally, we have

$$\begin{aligned}
x^{-1} y x &= y^k \\
x^{-2} y x^2 &= y^{k^2} \\
x^{-3} y x^3 &= y^{k^3}
\end{aligned}$$

Since $\operatorname{ord} x = 4$, we must have $y^{k^4} = y$, which implies $k^4 \equiv 1 \bmod 25$. Thus we see that

$$k \in \{1, 7, 18, 24\}.$$

Therefore we have the following isomorphism classes

$$\begin{aligned} G_1 &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y \rangle \\ G_7 &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^7 \rangle \\ G_{18} &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^{18} \rangle \\ G_{24} &= \langle x, y \mid x^4 = e, y^{25} = e, x^{-1}yx = y^{24} \rangle \end{aligned}$$

4.5 Problem 5

Exercise 19. Let $G = \mathrm{GL}_2(\mathbb{F}_5)$ and let $H = \mathrm{SL}_2(\mathbb{F}_5)$.

1. Show that G acts on H by conjugation. Prove any assumptions that you make along the way. You may of course assume properties of matrix multiplication and determinants.
2. Compute the stabilizers of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ under the action described above. What is the kernel of this action?

Solution 20. 1. Let $g \in G$ and $h \in H$. Then

$$\begin{aligned} \det(ghg^{-1}) &= \det(g)\det(h)\det(g)^{-1} \\ &= \det(g)\det(g)^{-1}\det(h) \\ &= \det(h) \\ &= 1, \end{aligned}$$

where we used the fact that $\det\colon \mathrm{GL}_2(\mathbb{F}_5) \to \mathbb{F}_5^\times$ is a group homomorphism. It follows that $ghg^{-1} \in H$, and hence H is a normal subgroup of G.

Thus we can define a map $\pi\colon G \times H \to H$, denoted $\pi(g,h) = g \cdot h$, by

$$g \cdot h = ghg^{-1}. \tag{23}$$

for all $g \in G$ and $h \in H$. We claim that π is an action of G on H. To see this, first note that π lands in H since H is a normal in G. Next, let $g_1, g_2 \in G$ and let $h \in H$. Then

$$\begin{aligned} g_1 \cdot (g_2 \cdot h) &= g_1 \cdot (g_2 h g_2^{-1}) \\ &= g_1(g_2 h g_2^{-1})g_1^{-1} \\ &= (g_1 g_2)h(g_1 g_2)^{-1} \\ &= (h_1 h_2) \cdot h. \end{aligned}$$

Also if $e \in G$ is the identity, then

$$\begin{aligned} e \cdot h &= ehe^{-1} \\ &= h. \end{aligned}$$

It follows that π is a group action of G on H.

2. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_5)$. We have

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff \begin{pmatrix} a+c & b+d-a-c \\ c & d-c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &\iff c = 0 \text{ and } d = a \end{aligned}$$

Thus

$$\begin{aligned}\mathrm{Stab}_G\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) &= \left\{\begin{pmatrix}a & b\\ 0 & a\end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_5)\right\}\\ &= \left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \mid b \in \mathbb{F}_5\right\} \cup \left\{\begin{pmatrix}4 & b\\ 0 & 4\end{pmatrix} \mid b \in \mathbb{F}_5\right\}.\end{aligned}$$

Similarly, we have

$$\begin{aligned}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix} &\iff \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\\ &\iff \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\\ &\iff \begin{pmatrix}-a & -b\\ c & d\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\\ &\iff \begin{pmatrix}a & -b\\ -c & d\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\\ &\iff b = -b \text{ and } c = -c\\ &\iff b = c = 0.\end{aligned}$$

Thus

$$\begin{aligned}\mathrm{Stab}_G\left(\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\right) &= \left\{\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_5)\right\}\\ &= \left\{\begin{pmatrix}a & 0\\ 0 & a^{-1}\end{pmatrix} \mid a \in \mathbb{F}_5^\times\right\}.\end{aligned}$$

The kernel of π is given by

$$\begin{aligned}\ker_G(H) &= \left\{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\right\}\\ &= \{g \in G \mid gh = hg \text{ for all } h \in H\}.\end{aligned}$$

Thus the kernel of π is the set of all elements in G which commute with every element in H. Clearly we have

$$\ker_G(H) \supseteq \left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix} \mid a \in \mathbb{F}_5\right\}.$$

In fact, we claim that the reverse inclusion holds too. Indeed, let $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in G$ and let $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in H$. We have

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

if and only if

$$\begin{pmatrix}a\alpha + b\gamma & a\beta + b\delta\\ c\alpha + d\gamma & c\beta + d\delta\end{pmatrix} = \begin{pmatrix}\alpha a + \beta c & \alpha b + \beta d\\ \gamma a + \delta c & \gamma b + \delta d\end{pmatrix}$$

if and only if

$$\begin{aligned}b\gamma &= \beta c\\ a\beta + b\delta &= \alpha b + \beta d\\ c\alpha + d\gamma &= \gamma a + \delta c.\end{aligned}$$

If $\alpha = \beta = \delta = 1$ and $\gamma = 0$, then we must have $c = 0$ and $a = d$. Similarly if $\alpha = \gamma = \delta = 1$ and $\beta = 0$, then we must have $b = 0$. It follows that any element in G which commutes with all elements in H must have the form $\left(\begin{smallmatrix}a & 0\\ 0 & a\end{smallmatrix}\right)$ for some $a \in \mathbb{F}_5$. Thus

$$\ker_G(H) = \left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix} \mid a \in \mathbb{F}_5\right\}.$$

5 Summer 2018

5.1 Abstract Algebra

5.1.1 Problem 1

Exercise 20. Let p be a positive prime integer. We consider S_p, the symmetric group on p elements.

1. How many elements of order p are there in S_p?
2. How many subgroups of order p are there?
3. What do the Sylow Theorems tell us about the possibilities for the number of p-Sylow subgroups of S_p?
4. For what value(s) of p is the p-Sylow subgroup of S_p a normal subgroup of S_p?
5. Wilson's Theorem implies that if p is a prime, then
$$(p-1)! \equiv -1 \mod p.$$
Use the previous results to prove this statement.

Solution 21. 1. An element σ in S_p has order p if and only if it is a cycle of length p. Thus we are counting the number of all p-cycles in S_p. Let X be the set of all p-cycles in S_p. Then S_p gives rise to an group action on X by conjugation: if $\sigma \in S_p$ and $(a_1 a_2 \cdots a_p) \in X$, then
$$\sigma(a_1 a_2 \cdots a_p)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_p)).$$
Note that the orbit of $(12\cdots p)$ under this action is all of X. Indeed, let $(a_1 a_2 \cdots a_p) \in X$ and let $\sigma = (1a_1)(2a_2)\cdots(pa_p)$. Then we have
$$\sigma(12\cdots p)\sigma^{-1} = (a_1 a_2 \cdots a_p).$$
Furthermore, we have $\sigma(12\cdots p)\sigma^{-1} = (12\cdots p)$ if and only if $\sigma = (12\cdots p)^k$ for some $1 \le k \le p$. Thus
$$\mathrm{Fix}_{S_p}((12\cdots p)) = \langle (12\cdots p)\rangle.$$
It follows from the orbit-stabilizer theorem that
$$\begin{aligned} |X| &= |\mathrm{Orb}_{S_p}((12\cdots p))| \\ &= |S_p|/|\mathrm{Fix}_{S_p}((12\cdots p))| \\ &= p!/p \\ &= (p-1)!. \end{aligned}$$

2. Let n denote the number of p-subgroups of S_p and let $H_1, \ldots, H_n$ denote the p-subgroups of S_p. Any group of order p is a cyclic group. In particular, each H_i consists of the identity element together with $p-1$ different p-cycles. Furthemore, for $i \neq j$, we have $H_i \cap H_j = \{1\}$. Thus we have
$$\begin{aligned} (p-1)! &= |(H_1\backslash\{1\} \cup \cdots \cup H_n\backslash\{1\}| \\ &= |(H_1\backslash\{1\}| + \cdots + |H_n\backslash\{1\}| \\ &= n(p-1). \end{aligned}$$
Therefore $n = (p-2)!$.

3. Let n_p denote number of p-Sylow subgroups of S_p. Observe that $|S_p| = p! = p(p-1)!$. Since $p \nmid (p-1)!$, it follows that the order of any p-Sylow subgroup of S_p is p. Thus the p-Sylows subgroups of S_p are precisely the p-subgroups. By the previous problem, we have $n_p = (p-2)!$. Now the Sylow Theorems tells us that
$$n_p \equiv 1 \mod p \qquad \text{and} \qquad n_p \mid (p-1)!.$$

4. Suppose S_p has a normal p-Sylow subgroup. Then necessarily we have $n_p = 1$. Since $n_p = (p-2)!$ (as counted above), this implies $p = 2$ or $p = 3$.

5. Combining the previous results, we have
$$(p-2)! = n_p \equiv 1 \mod p. \tag{24}$$
Multiplying both sides of (24) by $p-1$ gives us the desired result.

5.1.2 Problem 2

Exercise 21. Consider the ordinary integers $\mathbb{Z}$.

1. Show that every subgroup of $\mathbb{Z}$ is cyclic.
2. Show that every homomorphic image of $\mathbb{Z}$ is cyclic.
3. Use the previous to show that $\mathbb{Z}$ is a principal ideal domain.
4. Show that in a principal ideal domain, any two nonzero elements a and b have a greatest common divisor that is a linear combination of a and b.
5. Use the previous to show that every finitely generated, nonidentity subgroup of $\mathbb{Q}$ is isomorphic to $\mathbb{Z}$.

Solution 22. 1. Let A be a subgroup of $\mathbb{Z}$. Choose $a \in A\backslash\{0\}$ such that $|a|$ is minimal; that is, $b \in A\backslash\{0\}$ implies $|a| \leq |b|$. We claim that $A = \langle a \rangle$. Indeed, let $b \in A$. Since $\mathbb{Z}$ is a Euclidean domain, there exists $r, n \in \mathbb{Z}$ such that

$$b = na + r$$

where either $r = 0$ or $0 < |r| < |a|$. We claim that $r = 0$ (which will imply $b \in \langle a \rangle$). To see this, assume for a contradiction that $r \neq 0$, so $r < a$. Then note that $r = b - na$ implies $r \in A$. However this contradicts our choice of $a \in A$ with $|a|$ being minimal. Thus we must have $r = 0$, which implies $b \in \langle a \rangle$.

2. Let A be an abelian group and let $\varphi\colon \mathbb{Z} \to A$ be a surjective homomorphism. We claim that $A = \langle \varphi(1) \rangle$. Indeed, let $a \in A$. Choose $n \in \mathbb{Z}$ such that $\varphi(n) = a$ (we can do this since φ is surjective). Then we have

$$a = \varphi(n) = n\varphi(1).$$

Thus $A = \langle \varphi(1) \rangle$.

3. Let I be a subgroup of $\mathbb{Z}$. By 1, we know that every subgroup of $\mathbb{Z}$ is cyclic. In particular, I is cyclic. Thus I is generated by one element, which implies $\mathbb{Z}$ is a principal ideal domain. More generally, any Euclidean domain is a principal ideal domain.

4. Let R be a principal ideal domain and let $a, b \in R\backslash\{0\}$. Since R is a principal ideal domain, there exists a $d \in R$ such that

$$\langle a, b \rangle = \langle d \rangle. \tag{25}$$

Since $d \in \langle a, b \rangle$, there exists $x, y \in R$ such that

$$ax + by = d \tag{26}$$

Since $a, b \in \langle d \rangle$, there exists $\widetilde{a}, \widetilde{b} \in R$ such that

$$d\widetilde{a} = a \quad \text{and} \quad d\widetilde{b} = b$$

In particular, $d \mid a$ and $d \mid b$. Now suppose $d' \in R$ such that $d' \mid a$ and $d' \mid b$, say

$$d'a' = a \quad \text{and} \quad d'a' = b$$

where $a', b' \in R$. Then by (26), we have

$$\begin{aligned} d &= ax + by \\ &= d'a'x + d'b'y \\ &= d'(a'x + b'y). \end{aligned}$$

In particular, $d' \mid d$. Thus d is a greatest common divisor, and (26) shows that it is a linear combination of a and b.

5. Let A be a finitely generated, nonidentity subgroup of $\mathbb{Q}$. . Choose $b \in \mathbb{Z}$ such that $bA \subseteq \mathbb{Z}$. Then bA is a subgroup of $\mathbb{Z}$, and thus in particular, is it generated by one element, say $bA = \langle a \rangle$. It follows that $A = \langle a/b \rangle$.

6 Winter 2017

6.1 Problem 1

Exercise 22. Let F be a field, let $F^{n\times n}$ be the vector space of $n \times n$ matrices over F and let $\{E_{ij} \mid 1 \leq i, j \leq n\}$ be a basis of $F^{n\times n}$ consisting of matrices with an entry 1 in row i and column j and zero otherwise.

1. Show that the trace function $\mathrm{Tr}\colon F^{n\times n} \to F$ is a linear functional such that

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

   for all $A, B \in F^{n\times n}$.

2. Let $f\colon F^{n\times n} \to F$ be a linear functional such that

$$f(AB) = f(BA)$$

   for all $A, B \in F^{n\times n}$. Prove that

   (a) $f(E_{ij}) = 0$ for $1 \leq i < j \leq n$ and
   (b) $f(E_{ii}) = f(E_{11})$ for all $1 \leq i \leq n$.

3. Let $f\colon F^{n\times n} \to F$ be a linear functional. Prove that the following conditions on f are equivalent:

   (a) $f(AB) = f(BA)$ for every $A, B \in F^{n\times n}$.
   (b) There is $a \in F$ such that $f(C) = a\mathrm{Tr}(C)$ for all $C \in F^{n\times n}$.

Solution 23. 1. Let $A, B \in F^{n\times n}$ and let $a, b \in F$. Express A and B in matrix notation as

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

Then we have

$$\begin{aligned} \mathrm{Tr}(aA + bB) &= \mathrm{Tr}\left(a \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + b \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \right) \\ &= \mathrm{Tr} \begin{pmatrix} aa_{11} + bb_{11} & \cdots & aa_{1n} + bb_{1n} \\ \vdots & \ddots & \vdots \\ aa_{n1} + bb_{n1} & \cdots & aa_{nn} + bb_{nn} \end{pmatrix} \\ &= \sum_{i=1}^{n} aa_{ii} + bb_{ii} \\ &= a \sum_{i=1}^{n} a_{ii} + b \sum_{i=1}^{n} b_{ii} \\ &= a\mathrm{Tr}(A) + b\mathrm{Tr}(B). \end{aligned}$$

It follows that Tr is a linear functional. Also, we have

$$\begin{aligned}
\mathrm{Tr}(AB) &= \mathrm{Tr}\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}\right) \\
&= \mathrm{Tr}\begin{pmatrix} \sum_{i=1}^n a_{1i}b_{i1} & \cdots & \sum_{i=1}^n a_{1i}b_{in} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n a_{ni}b_{i1} & \cdots & \sum_{i=1}^n a_{ni}b_{in} \end{pmatrix} \\
&= \sum_{j=1}^n \sum_{i=1}^n a_{ji}b_{ij} \\
&= \sum_{j=1}^n \sum_{i=1}^n b_{ij}a_{ji} \\
&= \mathrm{Tr}\begin{pmatrix} \sum_{j=1}^n b_{1j}a_{j1} & \cdots & \sum_{i=1}^n b_{1j}a_{jn} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n b_{nj}a_{j1} & \cdots & \sum_{i=1}^n b_{nj}a_{jn} \end{pmatrix} \\
&= \mathrm{Tr}\left(\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\right) \\
&= \mathrm{Tr}(AB)
\end{aligned}$$

2. Let $1 \leq i < j \leq n$. We have

$$\begin{aligned}
f(E_{ij}) &= f(E_{ii}E_{ij}) \\
&= f(E_{ij}E_{ii}) \\
&= f(0) \\
&= 0.
\end{aligned}$$

Similarly, let $1 \leq i \leq n$. We have

$$\begin{aligned}
f(E_{ii}) &= f(E_{i1}E_{1i}) \\
&= f(E_{1i}E_{i1}) \\
&= f(E_{11}).
\end{aligned}$$

3. First suppose that $f(AB) = f(BA)$ for every $A, B \in F^{n\times n}$. Let $C = (c_{ij}) \in F^{n\times n}$. We have

$$\begin{aligned}
f(C) &= f\left(\sum_{1\leq i,j\leq n} c_{ij}E_{ij}\right) \\
&= \sum_{1\leq i,j\leq n} c_{ij}f(E_{ij}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{ii}) + \sum_{1\leq i<j\leq n} c_{ij}f(E_{ij}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{ii}) \\
&= \sum_{1\leq i\leq n} c_{ii}f(E_{11}) \\
&= f(E_{11})\mathrm{Tr}(C).
\end{aligned}$$

Thus, setting $a = f(E_{11})$, we see that $f(C) = a\mathrm{Tr}(C)$ for all $C \in F^{n\times n}$.

Conversely, suppose $f(C) = a\mathrm{Tr}(C)$ for all $C \in F^{n\times n}$ for some $a \in F$. Let $A, B \in F^{n\times n}$. Then

$$\begin{aligned} f(AB) &= a\mathrm{Tr}(AB) \\ &= a\mathrm{Tr}(BA) \\ &= f(BA). \end{aligned}$$

Thus $f(AB) = f(BA)$ for all $A, B \in F^{n\times n}$.

6.2 Problem 2

Exercise 23. Let G be a group of order 72, let P_2 be a Sylow 2-subgroup of G, and let P_3 be a Sylow 3-subgroup of G.

1. Prove that G is not simple.
2. Describe all abelian groups of order 72 up to isomorphism.
3. Describe all possibilities for P_3 up to isomorphism.
4. Assume that P_2 and P_3 are cyclic, and describe all possibilities for G up to isomorphism in the following cases
   (a) P_2 is a normal subgroup of G;
   (b) P_3 is a normal subgroup of G.

Solution 24. 1. Let n_p denote the number of p-Sylow subgroups of G. Note that $72 = 2^3 \cdot 3^2$, so by the Sylow theorems, we have

$$n_2 \equiv 1 \bmod 2 \quad \text{and} \quad n_2 \mid 9.$$

Similarly, we have

$$n_3 \equiv 1 \bmod 3 \quad \text{and} \quad n_3 \mid 8.$$

It follows that $n_2 \in \{1, 3, 9\}$ and $n_3 \in \{1, 4\}$. If $n_3 = 1$, then P_3 is a normal subgroup of G, so assume $n_3 = 4$. Let X_3 denote the set of 3-Sylow subgroups of G and define $\pi\colon G \to \mathrm{Sym}(X_3) \cong S_4$ by $g \mapsto \pi_g$ where

$$\pi_g(P) = gPg^{-1}$$

for all $P \in X_3$. Denote $K = \ker \pi$. Then G/K embeds into S_4, which implies $[G : K] \mid 24$, which implies $3 \mid |K|$. It follows that K is a nontrivial normal subgroup of G.

2. By the fundamental theorem of finite abelian groups, every abelian group of order 72 is isomorphic to one of the groups listed below:

$$C_2^3 \times C_3^2$$
$$C_2^3 \times C_9$$

$$C_2 \times C_3^2 \times C_4$$
$$C_2 \times C_4 \times C_9$$
$$C_8 \times C_3^2$$
$$C_8 \times C_9$$

3.

6.3 Problem 4

Exercise 24. Let G be a finite multiplicative group of 2×2 integer matrices.

1. Given $A \in G$, what can one prove about:
   (a) $\det A$ and $\operatorname{tr} A$?
   (b) the characteristic polynomial of A?
   (c) the eigenvalues of A? (Hint: don't forget to consider the non-real cases).
   (d) the Jordan canonical form of A?
   (e) the order of A?
2. Is A necessarily diagonalizable? Why or why not?
3. Find all possible groups G up to isomorphism.

Solution 25. 1. First we note that G is a finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$. In particular, if $C \in \mathrm{GL}_2(\mathbb{Q})$, then

$$CGC^{-1} = \left\{ CAC^{-1} \mid A \in G \right\}$$

is a conjugate subgroup of $\mathrm{GL}_2(\mathbb{Q})$, which itself is isomorphic to G. Furthermore, the characteristic polynomial of A, the determinant of A, the eigenvalues of A, the trace of A, and the order of A are invariant under conjugation.

Now let $\pi_A(X)$ denote the minimal polynomial of A over $\mathbb{C}$ and let $\chi_A(X)$ denote the characteristic polynomial of A. Since A satisfies $A^n - I = 0$, it follows that $\pi_A \mid X^n - 1$. The irreducible factors of $X^n - 1$ are the cyclotomic polynomials $\Phi_d(X)$ where $d \mid n$. Since π_A is not a unit, it follows that the irreducible factoriation of π_A consists of Φ_d for some of the d's which divide n. In particular, since $\pi_A \mid \chi_A$, we have $\deg \pi_A \leq 2$. The cyclotomic polynomials with degree ≤ 2 are given below

$$\begin{aligned}
\Phi_1(X) &= X - 1 \\
\Phi_2(X) &= X + 1 \\
\Phi_3(X) &= X^2 + X + 1 \\
\Phi_4(X) &= X^2 + 1 \\
\Phi_6(X) &= X^2 - X + 1.
\end{aligned}$$

In the the table below, we describe all possible cases for π_A together with the relevant data such as the rational canonical form of A, denoted A_{rat}, and the Jordan canonical form of A, denoted A_{jor}. After the table, we will also describe why the remaining cases for π_A do not work.

π_A	χ_A	$\det A$	$\operatorname{tr} A$	eigenvalues	ord A	A_{rat}	A_{jor}
$X-1$	$(X-1)^2$	1	2	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$X+1$	$(X+1)^2$	1	-2	-1	2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
$(X-1)(X+1)$	$(X-1)(X+1)$	-1	0	$1, -1$	2	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
X^2+X+1	X^2+X+1	1	-1	ζ_3, ζ_3^2	3	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{pmatrix}$
X^2+1	X^2+1	1	0	$i, -i$	4	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$
X^2-X+1	X^2-X+1	1	1	ζ_6, ζ_6^5	6	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^5 \end{pmatrix}$

Note that $\pi_A \neq (X-1)^2$, since in this case

$$A_{\mathrm{jor}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which has infinite order. Similarly, $\pi_A \neq (X+1)^2$, since in this case A has the form

$$A_{\text{jor}} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

which again has infinite order. Finally, note that in each case in the table above, A_{rat} has integer entries. Thus there is always a multiplicative group of 2×2 entries have A_{rat} as one of its elements, namely the cyclic group generated by A_{rat}. Thus all possibilities listed in the table above are realized.

Now let N denote the kernel of the determinant map (which is a homomorphism). So we have the following short exact sequence of groups

$$1 \to N \to G \xrightarrow{\det} \{\pm 1\} \to 1$$

To understand G, we first describe N. First note that N is a multiplicative subgroup of $\mathrm{SL}_2(\mathbb{Z})$. In particular, there is a natural homomorphism $\varphi\colon N \to \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ given by reducing matrix entries mod 3. We claim that φ is injective. Indeed, let $A \in \ker \varphi$. To show that A is identity matrix, we just need to show that $\operatorname{tr} A = 2$. Indeed, we already know that $\det A = 1$ since $A \in N$, and the identity matrix is the only matrix of with finite order in $\mathrm{GL}_2(\mathbb{Z})$ which has determinant 1 and trace 2. Now since $A \in \ker \varphi$, it must have the form

$$A = \begin{pmatrix} 1+3a & 3b \\ 3c & 1+3d \end{pmatrix}$$

where $a, b, c, d \in \mathbb{Z}$. Since $\det A = 1$, we must have

$$\begin{aligned} 1 &= (1+3a)(1+3d) - 9bc \\ &= 1 + 3d + 3a + 9ad - 9bc \\ &= 1 + 3(a+d) + 9(ad-bc), \end{aligned}$$

which implies $a + d = 3(bc - ad)$. Therefore

$$\begin{aligned} \operatorname{tr} A &= 2 + 3(a+d) \\ &= 2 + 9(bc-ad). \end{aligned}$$

In other words, $\operatorname{tr} A \equiv 2 \bmod 9$. Since the only possibilities for $\operatorname{tr} A$ are $\{-2,-1,0,1,2\}$, it follows that $\operatorname{tr} A = 2$, hence φ is injective.

In particular, N is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

7 Winter 2016

7.1 Problem 1

Exercise 25. Let V be a finite-dimensional real vector space. Let W_1 and W_2 be subspaces of V. We defined the following operations

$$(w_1, w_2) + (w_1', w_2') := (w_1 + w_1', w_2 + w_2') \quad \text{and} \quad \alpha(w_1, w_2) := (\alpha w_1, \alpha w_2)$$

for all $\alpha \in \mathbb{R}$, $w_1 \in W_1$, and $w_2 \in W_2$. The set $W_1 \times W_2$ is a vector space with respect to these operations.

1. Let $U = \{(u, -u) \mid u \in W_1 \cap W_2\}$. Prove that U is a subspace of $W_1 \times W_2$ isomorphic to $W_1 \cap W_2$.
2. Define the map $T\colon W_1 \times W_2 \to W_1 + W_2$ by $T(w_1, w_2) = w_1 + w_2$. Prove that T is a linear transformation.
3. Use the above to prove that

$$\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = \dim W_1 + \dim W_2.$$

Solution 26. 1. We first show U is a subspace of $W_1 \times W_2$. It is nonempty since $(0,0) \in U$. Let $\alpha, \alpha' \in \mathbb{R}$ and let $(u,-u), (u',-u') \in U$. Then observe that

$$\begin{aligned} \alpha(u,-u) + \alpha'(u',-u') &= (\alpha u + \alpha' u', -\alpha u - \alpha' u') \\ &= (\alpha u + \alpha' u', -(\alpha u + \alpha' u')) \\ &\in U, \end{aligned}$$

where the last part follows from the fact that $\alpha u + \alpha' u' \in W_1 \cap W_2$ since $W_1 \cap W_2$ is a subspace of V. It follows that U is a subspace of $W_1 \times W_2$. Let us now show that it is isomorphic to $W_1 \cap W_2$. Define $\varphi \colon U \to W_1 \cap W_2$ by

$$\varphi(u, -u) = u$$

for all $(u, -u) \in U$. Clearly φ is a bijection and a linear map, hence it is an isomorphism.

2. Let $\alpha, \alpha' \in \mathbb{R}$ and let $(w_1, w_2), (w_1', w_2') \in W_1 \times W_2$. Then we have

$$\begin{aligned} T(\alpha(w_1, w_2) + \alpha'(w_1', w_2')) &= T((\alpha w_1 + \alpha' w_1', \alpha w_2 + \alpha' w_2')) \\ &= \alpha w_1 + \alpha' w_1' + \alpha w_2 + \alpha' w_2' \\ &= \alpha(w_1 + w_2) + \alpha'(w_1' + w_2') \\ &= \alpha T(w_1, w_2) + \alpha' T(w_1', w_2'). \end{aligned}$$

It follows that T is a linear map.

3. First note that $\ker T = U$. Indeed, we have

$$\begin{aligned} T(w_1, w_2) = 0 &\iff w_1 + w_2 = 0 \\ &\iff w_1 = -w_2 \\ &\iff (w_1, w_2) \in U. \end{aligned}$$

Next we note that $\operatorname{im} T = W_1 + W_2$. Thus by the rank nullity theorem, we have

$$\begin{aligned} \dim W_1 + \dim W_2 &= \dim(W_1 \times W_2) \\ &= \dim(\ker T) + \dim(\operatorname{im} T) \\ &= \dim U + \dim(W_1 + W_2) \\ &= \dim(W_1 \cap W_2) + \dim(W_1 + W_2). \end{aligned}$$

7.2 Problem 2

Exercise 26. Let A and B be two real symmetric matrices. Show that they commute if and only if they are diagonalizable in a common orthonormal basis using the following path:

1. If A and B are diagonalizable in a common orthonormal basis, then A and B commute.
2. If A and B commute, and if λ is an eigenvalue of A, then the eigenspace E_λ of A that is associated to the eigenvalue λ is invariant under B.
3. If A and B commute, then A and B have at least one common eigenvector.
4. If A and B commute, then A and B are diagonalizable in a common orthonormal basis.

Solution 27. 1. Suppose A and B are diagonalizable in a common orthonormal basis, say

$$PAP^\top = D_1 \quad \text{and} \quad PBP^\top = D_2$$

where P is an orthonormal matrix whose column vectors correspond to a common eigenbasis. In particular $P^\top = P^{-1}$. Then we have

$$\begin{aligned} AB &= P^\top D_1 P P^\top D_2 P \\ &= P^\top D_1 D_2 P \\ &= P^\top D_2 D_1 P \\ &= P^\top D_2 P P^\top D_1 P \\ &= BA. \end{aligned}$$

Thus A and B commute.

2. Suppose A and B commute and let λ be an eigenvalue of A with corresponding eigenspace E_λ. Then for any eigenvector $v \in E_\lambda$ corresponding to the eigenvalue λ, we have

$$\begin{aligned} ABv &= BAv \\ &= B\lambda v \\ &= \lambda Bv. \end{aligned}$$

It follows that Bv is also an eigenvector corresponding to the eigenvalue λ. Thus E_λ is invariant under B.

3. Suppose A and B commute. Since $B \neq 0$, we must have $B|_{E_\lambda} \neq 0$ for some eigenvalue λ of A. Applying the real spectral theorem to $B|_{E_\lambda}$, we see that there exists an eigenvector $v \in E_\lambda$ for $B|_{E_\lambda}$. Since $B|_{E_\lambda}$ is just the restriction of B to E_λ, we see that v is an eigenvector for B, and since $v \in E_\lambda$, we see that v is an eigenvector for A too. Thus v is a common eigenvector of A and B.

4. It is easier to prove this in the setting where A and B are linear transformations from a finite dimensional Hilbert-space $(V, \langle \cdot, \cdot \rangle)$ to itself. In this case, A and B being symmetric in the old settting translates to A and B being self-adjoint in the new setting: that is

$$\langle Av, w \rangle = \langle v, Bw \rangle \quad \text{and} \quad \langle Bv, w \rangle = \langle v, Bw \rangle$$

for all $v, w \in V$. So assuming A and B commute, let us show that they are diagonalizable and have a common orthonormal basis. We will do this by induction on the dimension of V. The base case $n = 1$ is trivial. Assume that we have shown the proposition to be true for all self-adjoint commuting linear maps $A, B \colon V \to V$ for all finite-dimensional Hilbert spaces V where $\dim V < n$ for some $n > 1$. Now suppose $A, B \colon V \to V$ are self-adjoint linear maps and suppose $\dim V = n$. By part 3, A and B both have a common eigenvector, say v (necessarily $v \neq 0$). By rescaling if necessary, we choose v such that $\|v\| = 1$. Consider the subspace W of V defined by

$$W = \{w \in V \mid \langle w, v \rangle = 0\}.$$

Since the inner-product is positive-definite, we have $\langle v, v \rangle \neq 0$. Thus the map $\langle \cdot, v \rangle \colon V \to \mathbb{R}$ is onto, and since $\ker(\langle \cdot, v \rangle) = W$, we see that $\dim W = n - 1$. Now observe that $A|_W$ and $B|_W$ are self-adjoint commuting linear maps which act on a finite-dimensional Hilbert space of dimension $< n$. By induction, $A|_W$ and $B|_W$ share a common orthonormal eigenbasis, say $w_1, \ldots, w_{n-1} \in W$. We claim that $\{v, w_1, \ldots, w_{n-1}\}$ is a common orthonormal eigenbasis for both A and B. Indeed, it suffices to show that they form an orthonormal eigenbasis since v and w_i were chosen to be eigenvectors for both A and B. This follows immediately from the fact that $\langle v, w_i \rangle = 0$ for all $1 \leq i \leq n - 1$ since each $w_i \in W$. Also $\|v\| = \|w_i\| = 1$ for all $1 \leq i \leq n - 1$ by construction. Thus $\{v, w_1, \ldots, w_{n-1}\}$ is a common orthonormal eigenbasis for both A and B.

7.3 Problem 3

Exercise 27. Let G be a finite group.

1. Show that if $|G| = 2n$ with $n \geq 3$ then there is a nonabelian group of order $2n$.
2. Show that if $|G| = p$ with $p > 0$ a prime integer, then G is abelian.
3. Show that if $|G| = p^2$ with $p > 0$ a prime integer, then G is abelian.
4. Find the smallest odd integer n such that there is a nonabelian group of order n. Give generators and relations for such a group.

Solution 28. 1. Consider the Dihedral group D_n, given in terms of generators and relations by

$$D_n = \langle r, s \mid r^n = 1, s^n = 1, srs = r^{-1} \rangle.$$

Every element in D_n can be expressed in the form $r^i s^j$ for unique $0 \leq i \leq n - 1$ and $0 \leq j \leq 1$. In particular, $\#D_n = 2n$ (one can also see this from the isomorphism $D_n \cong C_2 \rtimes C_n$). Finally, we observe that D_n is nonabelian since in D_n we have $rs = r^{-1}s$. Thus r and s do not commute (if $rs = rs$, then we'd have $r = r^{-1}$ which is impossible since r has order > 2).

2. Suppose $\#G = p$. Choose any nonidentity element $g \in G$. Then by Lagrange's Theorem, we must have $\operatorname{ord} g \mid p$. This implies $\operatorname{ord} g = p$ since g is not the identity element and since p is prime. In particular, we see that G is a cyclic group (which is certainly abelian!).

3. To prove this, we use the following lemma:

Lemma 7.1. *Any p-group has nontrivial center.*

Proof. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|\mathrm{Z}(G)| = 1$. Let $x_1, \ldots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j}$ for each $1 \leq i < j \leq k$ and

$$G = \mathrm{Z}(G) \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{27}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (27) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction. □

Now we proceed with the problem at hand. Suppose $\#G = p^2$ and assume for a contradiction that $G \neq \mathrm{Z}(G)$. Since G is a p-group, $\mathrm{Z}(G)$ must be a nontrivial subgroup of G by Lemma (7.1). In particular, we must have $|\mathrm{Z}(G)| = p$. But then $|G/\mathrm{Z}(G)| = p$, which implies $G/\mathrm{Z}(G)$ is cyclic. It follows that G is abelian, which implies $G = \mathrm{Z}(G)$, a contradiction. So our assumption that $G \neq \mathrm{Z}(G)$ leads to a contradiction, which means we must in fact have $G = \mathrm{Z}(G)$.

7.4 Problem 4

Proposition 7.1. *Let A be a domain and let K be its quotient field. The following conditions are equivalent*

1. *For all nonzero $a, b \in A$, either $a \mid b$ or $b \mid a$;*
2. *For all nonzero $x \in K$, either x or x^{-1} is in A;*
3. *There is a valuation v on K such that $A = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$.*

Proof. ($1 \implies 2$): Let $x \in K^\times$. Write $x = a/b$ where $a, b \in A \backslash \{0\}$. Then either $a \mid b$ or $b \mid a$. If $b \mid a$, then we can write $a = bc$ for some nonzero $c \in A$. In this case, we have

$$\begin{aligned} x &= a/b \\ &= bc/b \\ &= c, \end{aligned}$$

and hence $x \in A$. On the other hand, if $a \mid b$, then we can write $b = ad$ for some nonzero $d \in A$. In this case, we have

$$\begin{aligned} x^{-1} &= b/a \\ &= ad/a \\ &= d, \end{aligned}$$

and hence $x^{-1} \in A$.

(2 $\implies$ 3): Let $\Gamma = K^\times / A^\times$. We define a total ordering on Γ as follows: Let $\overline{x}, \overline{y} \in \Gamma$. We say

$$\overline{x} \geq \overline{y} \text{ if and only if } xy^{-1} \in A. \tag{28}$$

Let us check that (28) is well-defined. Suppose xa and yb are two different representatives of the cosets $\overline{x}$ and $\overline{y}$ respectively, where $a, b \in A^\times$. Then

$$\begin{aligned}(xa)(yb)^{-1} &= (xa)(b^{-1}y^{-1}) \\ &= (xy^{-1})(ab^{-1}) \\ &\in A\end{aligned}$$

implies $\overline{xa} \geq \overline{yb}$. Thus (28) is well-defined. Next, observe that the relation given in (28) is antisymmetric: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{x}$, then $xy^{-1} \in A$ and $yx^{-1} \in A$, which implies $xy^{-1} \in A^\times$, and hence

$$\begin{aligned}\overline{x} &= \overline{x(yy^{-1})} \\ &= \overline{(xy^{-1})y} \\ &= \overline{y}.\end{aligned}$$

It is also transitive: if $\overline{x} \geq \overline{y}$ and $\overline{y} \geq \overline{z}$, then

$$\begin{aligned}xz^{-1} &= x(y^{-1}y)z^{-1} \\ &= (xy^{-1})(yz^{-1}) \\ &\in A,\end{aligned}$$

which implies $\overline{x} \geq \overline{z}$. It is also a total relation since either $\overline{x} \geq \overline{y}$ or $\overline{y} \geq \overline{x}$ (since either $xy^{-1} \in A$ or $yx^{-1} \in A$ by our assumption). Thus (28) gives us a total ordering on Γ.

Now we define $v \colon K^\times \to \Gamma$ to be the natural quotient map. Clearly v is a surjective homomorphism. We also have

$$v(x+y) \geq \min\{v(x), v(y)\} \text{ with equality if } v(x) \neq v(y).$$

Indeed, assume without loss of generality that $v(y) \geq v(x)$, so $v(x) = \min\{v(x), v(y)\}$. Then $(x+y)x^{-1} = 1 + yx^{-1} \in A$ implies $v(x+y) \geq v(x)$. Now assume $v(x) \neq v(y)$, so $yx^{-1} \notin A$. Then $x^{-1}(x+y) = 1 + yx^{-1} \notin A$. This implies $x(x+y)^{-1} \in A$ (by our assumption). Thus $v(x) \geq v(x+y)$, which implies $v(x) = v(x+y)$ by antisymmetry of $\geq$. Finally, we observe that

$$A^\times = \{x \in K \mid v(x) = 0\}$$

by construction. Moreover, we have

$$A = \{x \in K \mid v(x) \geq 0\} \cup \{0\},$$

since $v(x) \geq 0$ if and only if $v(x) \geq v(1)$ if and only if $x \in A$.

(3 $\implies$ 1): Let $(\Gamma, \geq)$ be a totally ordered abelian group and let $v \colon K^\times \to \Gamma$ be such a valuation. Suppose $a, b \in A \backslash \{0\}$, and without loss of generality, assume that $v(b) \geq v(a)$. Then

$$\begin{aligned}v(ba^{-1}) &= v(b) - v(a) \\ &\geq 0\end{aligned}$$

implies $ba^{-1} \in A$. In particular, this implies $a \mid b$. □

8 Winter 2014

8.1 Abstract Algebra

8.1.1 Problem 1

Exercise 28. Let p be a prime and $\mathbb{F}_p$ the finite field with p elements. Recall $\mathrm{GL}_n(\mathbb{F}_p)$ is the group of $n \times n$ intvertible matrices with entries in $\mathbb{F}_p$.

1. Prove that the size of $\mathrm{GL}_n(\mathbb{F}_p)$ is given by $\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=0}^{n-1}(p^n - p^j)$.

We now consider the case where $n = 2$. Set $G = \mathrm{GL}_2(\mathbb{F}_p)$, $U = \left\{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in G\right\}$, and $B = \left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G\right\}$.

2. Prove that U is a p-Sylow subgroup of G. Give another p-Sylow subgroup of G.

3. Prove that $B \subseteq \mathrm{N}_G(U)$ where $\mathrm{N}_G(U)$ denotes the normalizer of U in G.

4. Let n_p be the number of p-Sylow subgroups of G. Calculate n_p and prove your answer is correct.

Solution 29. 1. Let A be a random matrix in $\mathrm{GL}_n(\mathbb{F}_p)$ and let $v_1, \ldots, v_n$ denote the column vectors of A. Note that counting the number of matrices A in $\mathrm{GL}_n(\mathbb{F}_p)$ is equivalent to counting the number of ordered tuples of linearly independent vectors $(v_1, \ldots, v_n)$. So it suffices to count the latter.

There are $p^n - 1$ different possible vectors in $\mathbb{F}_p^n$ for which v_1 can be. The only vector which is not allowed is the zero vector. This is because the vectors $(v_1, \ldots, v_n)$ must be linearly independent, so no zero vectors allowed. Now we fix v_1. Then there are $p^n - p$ different possible vectors in $\mathbb{F}_p^n$ for which v_2 can be. Indeed, v_1 and v_2 must be linearly independent, so v_2 cannot equal to any vectors of the form av_1 where $a \in \mathbb{F}_p$. If we had fixed v_1 to be a different vector, then the same counting argument would apply, so altogether, the number of pairs of linearly independent vectors (v_1, v_2) is $(p^n - 1)(p^n - p)$.

More generally, for $1 \leq j \leq n$, if the vectors $v_1, \ldots, v_{j-1}$ are fixed, then there are $p^n - p^{j-1}$ different possible vectors in $\mathbb{F}_p^n$ for which v_j can be. Again, varying the vectors $v_1, \ldots, v_{j-1}$ to a new set of fixed vectors results in the same counting argument, so altogether the number of j-tuples of linearly independent vectors $(v_1, v_2, \ldots, v_j)$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{j-1})$. In particular, taking $j = n$ gives us

$$\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=1}^{n}(p^n - p^{j-1}) = \prod_{j=0}^{n-1}(p^n - p^j).$$

2. First note that $\#G = (p^2 - p)(p^2 - 1) = p(p-1)^2(p+1)$. In particular, the largest power of p in $\#G$ is simply p. Thus every p-Sylow subgroup of $\#G$ has size p. The set U certainly has size p since every element in U has the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathbb{F}_p$. To see that it is a p-Sylow subgroup then, we just need to show that it is a subgroup. It is clearly nonempty. Also, if $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ and $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ are two matrices in U, then

$$\begin{aligned} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix} \\ &\in U. \end{aligned}$$

It follows that U is a subgroup, and hence a p-Sylow subgroup of G. In fact, it is a cyclic, generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Another p-Sylow subgroup of G is obtained by simply taking the transpose of all matrices in U. Namely we set $U^\top = \left\{\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \in G\right\}$. Again, $U^\top$ has a size p and is a subgroup of G, so it is a p-Sylow subgroup of G. It is different from U becuase, $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in U^\top$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \notin U$.

3. Let $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in B$ and $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Then

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} &= \frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \\ &= \frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} d & ax-b \\ 0 & a \end{pmatrix} \\ &= \frac{1}{ad}\begin{pmatrix} ad & a^2x \\ 0 & ad \end{pmatrix} \\ &= \begin{pmatrix} 1 & (a/d)x \\ 0 & 1 \end{pmatrix} \\ &\in U. \end{aligned}$$

It follows that $B \subseteq \mathrm{N}_G(U)$.

4. By the Sylow Theorems, we have $n_p = [\mathrm{N}_G(U) : U]$. Also the size of B is given by $\#B = (p-1)^2 p$. Thus

$$\begin{aligned} n_p &= [\mathrm{N}_G(U) : U] \\ &= [\mathrm{N}_G(U) : B][B : U] \\ &= [\mathrm{N}_G(U) : B](p-1)^2 \end{aligned}$$

$$n_p = [\mathrm{N}_G(U) : U]$$

We claim that $\mathrm{N}_G(U) = B$. Indeed, we've already shown that $B \subseteq \mathrm{N}_G(U)$. Conversely, let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in U$. Then

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} &= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d-cx & -b+ax \\ -c & a \end{pmatrix} \\ &= \frac{1}{\Delta} \begin{pmatrix} \Delta - acx & a^2 x \\ c^2 x & \Delta + acx \end{pmatrix} \end{aligned}$$

where $\Delta = ad - bc$. Thus $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ conjugates $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ to another element of U if and only if $c = 0$, that is, if and only if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$. It follows that $\mathrm{N}_G(U) \subseteq B$. Therefore $\mathrm{N}_G(U) = B$. Finally, the number of matrices in B is given by $\#B = (p-1)^2 p$ since for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in B$, there $p-1$ different choices for a and d and there are p different choices b. It follows from the Sylow Theorems that

$$\begin{aligned} n_p &= [G : \mathrm{N}_G(U)] \\ &= [G : B] \\ &= \frac{p(p-1)^2(p+1)}{p(p-1)^2} \\ &= p+1. \end{aligned}$$

8.1.2 Problem 2

Exercise 29. As usual, let S_n denote the set of bijections from the set $[n] = \{1, \ldots, n\}$ to itself.

1. Show that as a group S_n is generated by transpositions. Be sure to prove *all* your assertions.
2. Cayley's Theorem states that any group is isomorphic to a permutation group. Prove from first principles that any group of order n is isomorphic to a subgroup of S_n.
3. Considering what you know about $n \times n$ elementary matrices action on GL_n, show that any group of order n can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{F}_2)$.

Solution 30. 1. We shall prove this in two steps.

Step 1: First we show that any element in S_n can be expressed as a product of disjoint cycles. Let $\sigma \in S_n$. We shall describe an algorithm which expresses σ as a product of disjoint cycles. In the first step of the algorithm, choose any $a_{1,1} \in [n]$. Let k_1 be the least nonnegative integer such that $\sigma^{k_1}(a_{1,1}) = a_{1,1}$. We denote $a_{1,i_1} = \sigma^{i_1 - 1}(a_{1,1})$ for each $1 \leq i_1 \leq k_1$. Observe that $1 \leq k_1 \leq n$ by the pigeonhole principle. Also observe that $a_{1,i_1} \neq a_{1,i_1'}$ whenever $i_1 \neq i_1'$. Indeed, if $a_{1,i_1} = a_{1,i_1'}$ for some $1 \leq i_1 < i_1' \leq k_1$, then

$$\begin{aligned} \sigma^{i_1' - i_1}(a_{1,1}) &= \sigma^{i_1'} \sigma^{-i_1}(a_{1,1}) \\ &= \sigma^{-i_1} \sigma^{i_1'}(a_{1,1}) \\ &= \sigma^{-i_1}(a_{1,i_1'}) \\ &= \sigma^{-i_1}(a_{1,i_1}) \\ &= a_{1,1}, \end{aligned}$$

which would contradict the minimality of k_1 since $i_1' - i_1 < k_1$. So if we denote $\tau_1 = (a_{1,1} \cdots a_{1,k_1})$ and $\sigma_1 = \tau_1^{-1}\sigma$, then we can express σ as

$$\sigma = \tau_1\sigma_1.$$

where τ_1 is a cycle of length k_1 and where σ_1 fixes $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Indeed, we have

$$\begin{aligned}\sigma_1(a_{1,i}) &= \tau_1^{-1}\sigma(a_{1,i_1}) \\ &= \tau_1^{-1}(a_{1,i_1+1}) \\ &= a_{1,i_1},\end{aligned}$$

where a_{1,i_1+1} is understood to be $a_{1,1}$ if $i_1 = k_1$.

Now we proceed to the second step of the algorithm. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_1 is the identity element since it fixes all of $[n]$. Then $\sigma = \tau_1$ shows that σ is a cycle itself. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} \subset n$, where the inclusion is proper, then we choose any $a_{2,1} \in [n]\backslash\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Let k_2 be the least nonnegative integer such that $\sigma^{k_2}(a_{2,1}) = a_{2,1}$. We denote $a_{2,i_2} = \sigma^{i_2-1}(a_{2,1})$ for each $1 \leq i_2 \leq k_2$. As in the case of the first step of the algorithm, we observe that $1 \leq k_2 \leq n - k_1$ and we also observe that $a_{2,i_2} \neq a_{2,i_2'}$ whenever $i_2 \neq i_2'$. The proof for these two observations is nearly identical to the ones we did above. We denote $\tau_2 = (a_{2,1} \cdots a_{2,k_2})$ and $\sigma_2 = \tau_2^{-1}\sigma_1$. Then we can express σ_1 as

$$\sigma_1 = \tau_2\sigma_2,$$

where τ_2 is a cycle of length k_2 and where σ_2 fixes $\{a_{1,i_1}, a_{1,i_2} \mid 1 \leq i_1 \leq k_1 \text{ and } 1 \leq i_2 \leq k_2\}$. Indeed, the proof that σ_2 fixes a_{1,i_2} is nearly identical to the proof that σ_1 fixes a_{1,i_1}, and the reason that σ_2 fixes a_{1,i_1} is because both τ_2 and σ_1 fix a_{1,i_1}.

Now we describe the algorithm at the sth step where $s \geq 2$. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_{s-1} is the identity element since it fixes all of $[n]$. Then

$$\begin{aligned}\sigma &= \tau_1\sigma_1 \\ &= \tau_1\tau_2\sigma_2 \\ &\vdots \\ &= \tau_1\tau_2 \cdots \tau_{s-1}\sigma_{s-1} \\ &= \tau_1\tau_2 \cdots \tau_{s-1}\end{aligned}$$

shows that σ is a product of distinct cycles. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} \subset [n]$, where the inclusion is proper, then we choose any $a_{s,1} \in [n]\backslash\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$. Let k_s be the least nonnegative integer such that $\sigma^{k_s}(a_{s,1}) = a_{s,1}$. We denote $a_{s,i_s} = \sigma^{i_s-1}(a_{s,1})$ for each $1 \leq i_s \leq k_s$. As in the case of the first and second step of the algorithm, we observe that $1 \leq k_s \leq n - k_1 - \cdots - k_{s-1}$ and we also observe that that $a_{s,i_s} \neq a_{s,i_s'}$ whenever $i_s \neq i_s'$. We denote $\tau_s = (a_{s,1} \cdots a_{s,k_s})$ and $\sigma_s = \tau_s^{-1}\sigma_{s-1}$. Then we can express σ_{s-1} as

$$\sigma_{s-1} = \tau_s\sigma_s,$$

where τ_s is a cycle of length k_s and where σ_s fixes $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$.

This algorithm must terminate since $[n]$ is finite and since after the sth step, we produce a strictly increasing sequence of sets

$$(\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\})$$

each of which is contianed in $[n]$.

Step 2: Now we show that any cycle in S_n can be expressed as a product of transposition. Let $(a_1a_2 \cdots a_k)$ be any in S_n. We claim that

$$(a_1a_2 \cdots a_k) = \prod_{i=1}^{k-1}(a_ia_{i+1}). \tag{29}$$

Indeed, let $a \in [n]$. If $a \neq a_j$ for any $1 \leq j \leq k$, then applying a to both $(a_1a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ results in a again. In other words, both $(a_1a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ fix a. If $a = a_j$ for some $1 \leq j \leq k$, then applying a_j to

$(a_1a_2\cdots a_k)$ results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j=k$. Applying a_j to $\prod_{i=1}^{k-1}(a_ia_{i+1})$ also results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j=k$. Indeed,

$$\begin{aligned}\prod_{i=1}^{k-1}(a_ia_{i+1})(a_j) &= (a_1a_2)\cdots(a_{j-1}a_j)(a_ja_{j+1})\cdots(a_ka_{k-1})(a_j)\\ &= (a_1a_2)\cdots(a_{j-1}a_j)(a_ja_{j+1})(a_j)\\ &= (a_1a_2)\cdots(a_{j-1}a_j)(a_{j+1})\\ &= a_{j+1}.\end{aligned}$$

Combining step 1 with step 2 shows that any permutation can be expressed as a product of transpositions.

2. We state and prove Cayley's Theorem:

Theorem 8.1. *(Cayley's Theorem) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.*

Proof. We write S_G for the group of all permutations of G as a set. We have $S_G \cong S_n$, so we just need to show that G is isomorphic to a subgroup of S_G. Define a map $\pi\colon G \to S_G$, denoted $\pi \mapsto \pi_g$, where $\pi_g\colon G \to G$ is given by

$$\pi_g(x) = gx$$

for all $x \in G$. We claim that π is an injective group homomorphism. Indeed, first let us show that it is a group homomorphism. Let $g_1, g_2 \in G$. Then observe that

$$\begin{aligned}\pi_{g_1g_2}(x) &= g_1g_2x\\ &= \pi_{g_1}(g_2x)\\ &= \pi_{g_1}\pi_{g_2}(x)\end{aligned}$$

for all $x \in G$. It follows that $\pi_{g_1g_2} = \pi_{g_1}\pi_{g_2}$, and hence π is a group homomorphism. Now let us show that it is injective. Suppose $g \in \ker\pi$. Thus $gx = x$ for all $x \in G$. In particular, $g^2 = g$. Multiplying both sides by g^{-1} implies $g = 1$. Thus $\ker\pi = \{1\}$, which implies π is injective. Finally, by the first isomorphism theorem for groups, we find that $\operatorname{im}\pi$ is a subgroup of S_G, and moreover,

$$\operatorname{im}\pi \cong G/\ker\pi \cong G.$$

It follows that G is isomorphic to a subgroup of S_G which implies G is isomorphic to a subgroup of S_n.

□

3. It suffices to show that S_n can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{F}_2)$ since G can be realized as a subgroup of S_n. Since S_n is generated by transpositions, we can define a group homomorphism out of S_n by describing how it acts on transpositions, however we need to be sure that this map respects any relations involving these transpositions. For each $1 \le i < j \le n$, let s_{ij} be the matrix in $\mathrm{GL}_n(\mathbb{F}_2)$ obtained by swapping the ith row with the jth row in the identity matrix. For any matrix A, multiplying s_{ij} to left of A results in the same matrix obtained by swapping the ith and jth row of A. Thus we can view s_{ij} as a transposition of the rows of A. Thus we have the relations

$$s_{ij}s_{kl} = \begin{cases} s_{kl}s_{ij} & \text{if } i \neq k \text{ and } j \neq l\\ s_{kl}s_{il} & \text{if } j = k\\ s_{kl}s_{jl} & \text{if } i = k \text{ and } j \neq l\\ 1 & \text{if } i = k \text{ and } j = l\end{cases}$$

In particular, we can define an injective group homomorphism $\varphi\colon S_n \to \mathrm{GL}_n(\mathbb{F}_2)$ as follows: let $\sigma \in S_n$ and express it as a product of transpositions, say $\sigma = (i_1j_1)\cdots(i_kj_k)$. Then we set

$$\varphi(\sigma) = s_{i_1j_1}\cdots s_{i_kj_k}.$$

Note that φ is a well-defined group homomorphism since the s_{ij} satisfy the relations described above.

8.1.3 Problem 3

Exercise 30. Suppose that p is a prime and that R is a characteristic p ring which identity. Let

$$R\{X\} = \left\{ \sum_{i=0}^{n} a_i X^{p^i} \mid a_i \in R \right\} \tag{30}$$

Note that the polynomials in $R\{X\}$ have no constant term.

1. Show that $R\{X\}$ is a ring under the operations of polynomial addition and composition of functions.
2. Suppose that F is a characteristic p field. Then we can consider the ring $F\{X\}$ defined as in (30). It is a fact (which you do not need to prove) that $F\{X\}$ is not commutative. Show that $F\{X\}$ has a right division algorithm, that is, show that for $a(X), b(X) \in R\{X\}$ with $b(X) \neq 0$, there exists $q(X), r(X) \in F\{X\}$ with $r(X) = 0$ or $\deg(r(X)) < \deg(b(X))$ and $a(X) = q(X)b(X) + r(X)$.
3. Again suppose that F is a characteristic p field and consider the ring $F\{X\}$ defined as in (30). Show that every left ideal of $F\{X\}$ is principal. You may use the result from part (3b).

Solution 31. 1. Let $f, g, h \in R\{X\}$ and express them as

$$f(X) = \sum_{i \geq 0} a_i X^{p^i}, \quad g(X) = \sum_{i \geq 0} b_i X^{p^i}, \quad \text{and} \quad \sum_{i \geq 0} c_i X^{p^i}$$

where $a_i, b_i, c_i \in R$ such that $a_i = b_i = c_i = 0$ for $i \gg 0$. We have

$$\begin{aligned} f \circ g &= \sum_{i \geq 0} a_i \left(\sum_{j \geq 0} b_j X^{p^j} \right)^{p^i} \\ &= \sum_{i \geq 0} a_i \sum_{j \geq 0} b_j^{p^i} X^{p^{i+j}} \\ &= \end{aligned}$$

$$\begin{aligned} (f+g) \circ h &= \left(\sum_{i \geq 0} a_i X^{p^i} + \sum_{i \geq 0} b_i X^{p^i} \right) \sum_{i \geq 0} c_i X^{p^i} \\ &= \sum_{i \geq 0} (a_i + b_i) X^{p^i} \sum_{i \geq 0} c_i X^{p^i} \end{aligned}$$

8.2 Linear Algebra

8.2.1 Problem 3

Exercise 31. Let A be a real $n \times n$ matrix.

1. Prove that $\operatorname{rank}(A^{n+1}) = \operatorname{rank}(A^n)$.
2. Prove that $\operatorname{rank}(A^\top A) = \operatorname{rank}(A)$.
3. We say A is a **difference of two squares** if there exists real $n \times n$ matrices B and C such that $BC = CB = 0$ and $A = B^2 - C^2$. Prove that if A is symmetric, then A is a difference of two squares.
4. Let $A = B^2 - C^2$ be a difference of two squares as defined in part 3. Prove that if B has a nonzero real eigenvalue, then A has a positive real eigenvalue.

Solution 32. 1. First note that for any $i \in \mathbb{N}$, if $\dim(\operatorname{im} A^i) = \dim(\operatorname{im} A^{i+1})$, then $\operatorname{im} A^i = \operatorname{im} A^{i+1}$. Indeed, this is because $\operatorname{im} A^{i+1}$ is already a subspace of $\operatorname{im} A^i$, and so having equal dimensions forces equality. Now observe that

$$n \geq \dim(\operatorname{im} A) \geq \dim(\operatorname{im} A^2) \geq \cdots \geq \dim(\operatorname{im} A^i) \geq \cdots \geq 0.$$

By the pigeonhole principle, there must be some $1 \leq i \leq n$ such that $\dim(\operatorname{im} A^i) = \dim(\operatorname{im} A^{i+1})$. In this case, it follows that

$$\operatorname{im} A^i = \operatorname{im} A^{i+1} = \cdots = \operatorname{im} A^{n+1}.$$

In particular, we have $\operatorname{rank}(A^{n+1}) = \operatorname{rank}(A^n)$.

2. We claim that $A^\top|_{\operatorname{im} A} \colon \operatorname{im} A \to \operatorname{im} A^\top A$ is injective. Indeed, let $Av \in \ker A^\top$. Then observe that

$$\begin{aligned} \|Av\|^2 &= (Av)^\top (Av) \\ &= v^\top A^\top Av \\ &= v^\top 0 \\ &= 0, \end{aligned}$$

where $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^n$. Since $\|\cdot\|$ is positive definite, it follows that $Av = 0$. This implies $A^\top|_{\operatorname{im} A}$ is injective. Therefore

$$\begin{aligned} \operatorname{rank}(A^\top A) &= \dim(\operatorname{im}(A^\top A)) \\ &= \dim(\operatorname{im} A) \\ &= \operatorname{rank}(A). \end{aligned}$$

3. Assume that A is symmetric. By the real spectral theorem, A can be diagonalized by an orthogonal matrix. That is, there is an orthogonal matrix P and a diagonal matrix D such that $PAP^\top = D$. The diagonal matrix D has the form

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_k & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{k+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_n \end{pmatrix}$$

ordered in such a way that first k entries along the main diagonal are nonnegative and the remaining entries negative. Note that we can express D as $D = D_+^2 - D_-^2$ where

$$D_+ = \begin{pmatrix} \sqrt{\lambda_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\lambda_k} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad D_- = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{-\lambda_{k+1}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{-\lambda_n} \end{pmatrix}.$$

Furthermore it's easy to see that $D_+D_- = 0 = D_-D_+$. Then setting $B = P^\top D_+ P$ and $C = P^\top D_- P$, we find that

$$\begin{aligned} A &= P^\top DP \\ &= P^\top (D_+^2 - D_-^2) P \\ &= P^\top D_+^2 P - P^\top D_-^2 P \\ &= (P^\top D_+ P)^2 - (P^\top D_- P)^2 \\ &= B^2 - C^2. \end{aligned}$$

Furthemore we have

$$\begin{aligned} BC &= P^\top D_+ P P^\top D_- P \\ &= P^\top D_+ D_- P \\ &= P^\top 0 P \\ &= 0. \end{aligned}$$

A similar calculation gives us $CB = 0$.

4. Let λ be a nonzero eigenvalue for B and choose an eigenvector v corresponding to λ. Observe that

$$\begin{aligned} 0 &= CBv \\ &= \lambda Cv \end{aligned}$$

implies $Cv = 0$ since $\lambda \neq 0$. Therefore

$$\begin{aligned} Av &= (B^2 - C^2)v \\ &= B^2 v - C^2 v \\ &= B^2 v \\ &= \lambda^2 v. \end{aligned}$$

It follows that v is an eigenvector for A corresponding to the positive eigenvalue λ^2.