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 $\operatorname{Hom}_{\mathbb{R}}(W, V)$ denote the set of linear transformations $W \to V$, which is a real vector space.

1. Let $z \in \mathbb{C}$ and $\phi \in \operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. 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 $z\phi \in \operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

2. Prove that $\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is a complex vector space using (6) to define scalar multiplication.

3. Prove that if $d = \dim_{\mathbb{R}}(V) < \infty$, then $\dim_{\mathbb{C}}(\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.

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 $\mathbf{e} \otimes \mathbf{v} = (e_1v_1, \ldots, e_1v_n, e_2v_1, \ldots, e_2v_n, \ldots, e_mv_1, \ldots, e_mv_n)$ 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
$$v = b_1v_1 + \cdots + b_nv_n$$

for some $b_1, \dots, b_n \in L$. 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 $a_{1j}, \dots, a_{mj} \in K$. Therefore, we have

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

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

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

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

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 3. 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 3. 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 4. 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 4. 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

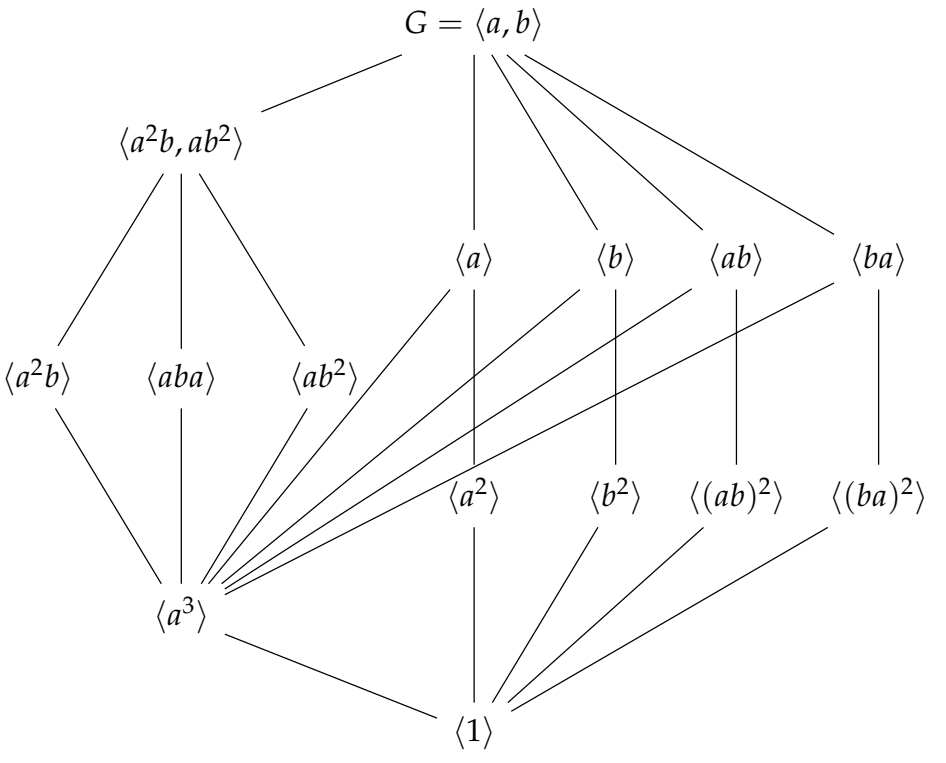
$$\begin{aligned} S \cap \left(\bigcup_{\lambda \in \Lambda} I_\lambda \right) &= \bigcup_{\lambda \in \Lambda} (S \cap I_\lambda) \\ &= \bigcup_{\lambda \in \Lambda} \emptyset \\ &= \emptyset. \end{aligned}$$

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 5. 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 5. 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.

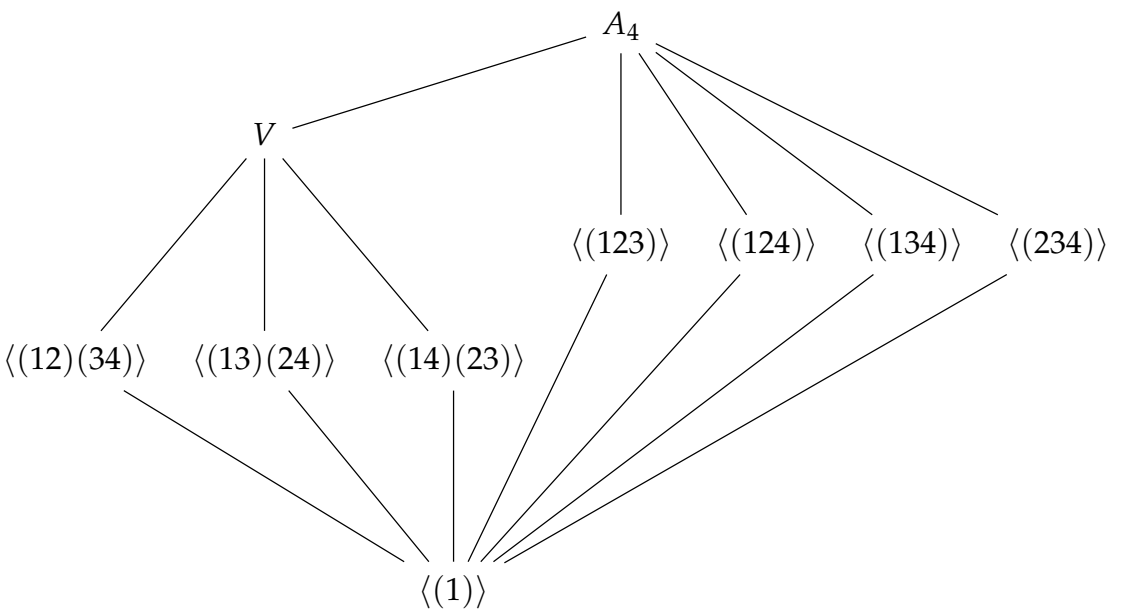
Equivalence Classes of Subgroups by Conjugacy
$\langle a \rangle$, $\langle b \rangle$, $\langle ab \rangle$, $\langle ba \rangle$
$\langle a^2 \rangle$, $\langle b^2 \rangle$, $\langle (ab)^2 \rangle$, $\langle (ba)^2 \rangle$
$\langle a^3 \rangle$
$\langle a^2b \rangle$, $\langle aba \rangle$, $\langle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

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

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

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.

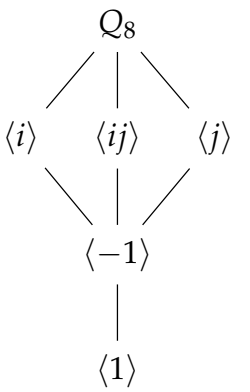


where $V = \langle(12)(34), (14)(23)\rangle$.

5. The group $\langle a^2b, ab^2\rangle$ 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 $\langle a^2b, ab^2\rangle$ is given by $a^2b \mapsto i$ 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 6. Fix an integer $d \geq 2$ and consider the real vector space

$$V_d = \mathbb{R}[x]_{<d} = \{a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} \mid a_0, \ldots, a_{d-1} \in \mathbb{R}\}.$$

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 $D^*(a_0 + a_1 x + \cdots + a_{d-1}x^{d-1})$ where $D^* \colon V \to V$ is the adjoint of D.

Solution 6. 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

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

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 7. 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 7. 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 8. 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 8. 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 9. 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 9. 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 10. (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

$$\begin{aligned}\overline{\varphi}(\overline{g}_1\overline{g}_2) &= \varphi(g_1g_2)\\ &= \varphi(g_1)\varphi(g_2)\\ &= \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).\end{aligned}$$

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 10. 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 11. 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 $\mathrm{N}(\alpha) = 1$, 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 $\mathrm{N}(a) \mid 4$ 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 $\mathrm{N}(a) \mid 9$ 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 2018

3.1 Problem 1

Exercise 11. 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 12. 1. 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

$$(X - \lambda_1)(X - \lambda_2)(X - \lambda_3) = \chi_A(X) = X^3 - (a^2 + b^2 + c^2)X - 2abc. \tag{21}$$

Expanding the product on the left side in (21) 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 $\lambda_1, \lambda_2 < 0$.

3.2 Problem 2

Exercise 12. 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 13. 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 $u + v \in \ker \mathrm{P}_W \mathrm{P}_U$.

3.3 Problem 3

Exercise 13. 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 14. 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.

3.4 Problem 4

Exercise 14. 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 15. 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 the 5-Sylow subgroup of G. Since $n_5 = 1$, it follows that P is a normal subgroup of G (conjugation P results in another 5-Sylow subgroup, which must be P). Any group whose order is p^2 for a prime p is abelian. In particular, P is an abelian group.

Now observe that $|G/P| = 4$. There are only two groups of order 4, namely C_4 and $C_2 \times C_2$. It follows that either $G/P \cong C_4$ or $G/P \cong C_2 \times C_2$. First assume that $G/P \cong C_4$. Let $x \in G$ be a representative of the coset which generates G/P. Then every element in G can be expressed in a unique way as $x^i y$ where $0 \leq i \leq 3$ and $y \in P$. Let $x^i y$ and $x^{i'} y'$ be any two elements in G. Then

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

$$n_5 \equiv 1$$

$$n_2 \in \{1, 5, 25\} \quad \text{and} \quad n_5 = 1$$

2.

3.

4 Summer 2018

4.1 Abstract Algebra

4.1.1 Problem 1

Exercise 15. 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 16. 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
$$(p-2)! = n_p \equiv 1 \mod p. \tag{22}$$
Multiplying both sides of (22) by $p-1$ gives us the desired result.

4.1.2 Problem 2

Exercise 16. 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 17. 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

$$\langle a, b \rangle = \langle d \rangle. \tag{23}$$

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

$$ax + by = d \tag{24}$$

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 (24), 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 (24) 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 $A = \langle a/b \rangle$.