Abstract Algebra Homework

Variously Kenneth Brown, Bryan Hanson, Jing Liu,
Austin Mohr, Ranil Wanigasiri, Pam Welch

April 26, 2012

Problem 0

Classify up to similarity all the square matrices over the complex numbers with minimal polynomial $m(x) = (x-1)^2(x-2)^2$ and characteristic polynomial $c(x) = (x-1)^6(x-2)^5$.

Let A be a matrix of the desired form. Observe first that, since we are working over $\mathbb{C}$, A can be expressed in Jordan form. Now, the roots of $c(x)$ are precisely the eigenvalues of A. Furthermore, a root's multiplicity in $m(x)$ gives the size of the largest elementary Jordan block in A. Since, up to similarity, permutations of the blocks are irrelevant, we have the following possibilities for A:

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

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

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

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

$$\begin{pmatrix}
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & & & & & \\
 & & & & 2 & & & &
\end{pmatrix}$$

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

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

Problem 1

Let $T : V \to V$ be a linear transformation of rank 1 on a finite dimensional vector space V over any field. Prove that either T is nilpotent or V has a basis of eigenvectors of T.

Proof. Let $dim(V) = n$ and let $\{\vec{v_0}\}$ be a basis for $R(T)$ (since $rank(T) = 1$). Observe that $\vec{v_0} = T(\vec{v_0'})$ for some $\vec{v_0'} \in V$. By the dimension theorem, the nullity of T is $n-1$, and so let $\{\vec{w_0}, \cdots, \vec{w_{n-2}}\}$ be a basis for $N(T)$.

Observe that, since $T \neq 0$, it cannot be that T is nilpotent *and* V has a basis of eigenvectors of T.

Suppose T is not nilpotent. We claim that $\{\vec{v_0}, \vec{w_0}, \cdots, \vec{w_1}\}$ is a basis of eigenvectors for V. Since T is not nilpotent, we have that $T(\vec{v_0}) = T^2(\vec{v_0'}) \neq 0$. Since T has rank 1, it must be that $T(\vec{v_0}) = \lambda\vec{v_0}$ for some $\lambda \neq 0$. In other words, $\vec{v_0}$ is an eigenvector for T. Now, $T(\vec{w_i}) = 0\vec{w_i}$ for all i, and so each $\vec{w_i}$ is an eigenvector for T with eigenvalue 0.

Now, the set $\{\vec{w_0}, \cdots, \vec{w_{n-2}}\}$ is independent, since it is a basis for $N(T)$. Suppose $\vec{v_0}$ can be expressed as a linear combination of the $\vec{w_i}$. Then

$$\begin{aligned} \vec{v_i} &= \sum_{i=0}^{n-2} a_i\vec{w_i} \\ T(\vec{v_i}) &= T(\sum_{i=0}^{n-2} a_i\vec{w_i}) \\ T(\vec{v_i}) &= \sum_{i=0}^{n-2} a_i T(\vec{w_i}) \\ T(\vec{v_i}) &= 0 \end{aligned}$$

which is a contradiction. Hence, $\{\vec{v_0}, \vec{w_0}, \cdots, \vec{w_{n-2}}\}$ is an independent set of n eigenvectors of T, and so a basis for V. □

Problem 2

Let V be a vector space over a field K.

a. Prove that if U_0 and U_1 are subspaces of V such that $U_0 \not\subseteq U_1$ and $U_1 \not\subseteq U_0$, then $V \neq U_0 \cup U_1$.

Proof. Since $U_0 \not\subseteq U_1$, there exists a basis vector $U_0 \ni \vec{u_0} \notin U_1$. Similarly, since $U_1 \not\subseteq U_0$, there exists a basis vector $U_0 \ni \vec{u_1} \notin U_1$. Now, consider the linear combination $\vec{u_0} + \vec{u_1} \in V$.

$\vec{u_0} + \vec{u_1} \notin U_0$ (since $\vec{u_0} \notin U_0$)

$\vec{u_0} + \vec{u_1} \notin U_1$ (since $\vec{u_1} \notin U_1$)

Hence, $\vec{u_0} + \vec{u_1} \notin U_0 \cup U_1$, and so $U_0 \cup U_1 \neq V$. □

b. Prove that if U_0, U_1, and U_2 are subspaces of V such that $U_i \not\subseteq U_j$ when $i \neq j$ and K has at least 3 elements, then $V \neq U_0 \cup U_1 \cup U_2$.

Proof. Since no subspace is contained in any other, we can find basis vectors $\vec{u_0} \notin U_0$, $\vec{u_1} \notin U_1$, and $\vec{u_2} \notin U_2$, $\vec{u_i} \in V$. Observe that if all the $\vec{u_i}$ are identical, then we have found a vector in V which is in none of the U_i, and so $U_0 \cup U_1 \cup U_2 \neq V$. Let it be, instead, that at least one of the $\vec{u_i}$ differs from the rest. Without loss of generality, let $\vec{u_0}$ differ from the rest of the $\vec{u_i}$. Now, consider the linear combination $\vec{u_0} + \vec{u_1} + \vec{u_2} \in V$. It is possible that $\vec{u_1} = \vec{u_2}$, but since K is of characteristic 3, we are assured that $\vec{u_1} + \vec{u_2} \neq 0$. It follows that, for all i $\quad \vec{u_0} + \vec{u_1} + \vec{u_2} \notin U_i$ (since $\vec{u_i} \notin U_i$)

Hence, $\vec{u_0} + \vec{u_1} + \vec{u_2} \notin U_0 \cup U_1 \cup U_2$, and so $U_0 \cup U_1 \cup U_2 \neq V$. □

c. State a prove a generalization of (b) for n subspaces.

Proposition 1. *Let V be a finite-dimensional vector space over a field K of characteristic at least n. Let $\{U_i \mid 0 \leq i \leq n-1\}$ be a set of subspaces such that $U_i \not\subseteq U_j$ for $i \neq j$. Then,*

$$\bigcup_{i=0}^{n-1} U_i \neq V$$

Proof. Since no subspace is contained in any other, we can find basis vectors $V \ni \vec{u_i} \notin U_i$ for each $0 \leq i \leq n-1$. Observe that if all the $\vec{u_i}$ are identical, then we have found a vector in V which is in none of the U_i, and so $\bigcup_{i=0}^{n-1} U_i \neq V$. Let it be, instead, that at least one of the $\vec{u_i}$ differs from the rest. Without loss of generality, let $\vec{u_0}$ differ from the rest of the $\vec{u_i}$. Now, consider the linear combination $\sum_{i=0}^{n-1} \vec{u_i} \in V$. It is possible that $\vec{u_1} = \vec{u_2} = \cdots = \vec{u_{n-1}}$,

but since K is of characteristic n, we are assured that $\sum_{i=1}^{n-1} \vec{u_i} \neq 0$. It follows that, for all $0 \leq j \leq n-1$

$$\sum_{i=0}^{n-1} \vec{u_i} \notin U_j \text{ (since } \vec{u_j} \notin U_j)$$

Hence,

$$\sum_{i=0}^{n-1} \vec{u_i} \notin \bigcup_{i=0}^{n-1} U_i$$

and so $\bigcup_{i=0}^{n-1} U_i \neq V$. □

For the following problems, let

$$\mathbf{A} = \langle A, *_i \rangle$$
$$\mathbf{B} = \langle B, \Box_i \rangle$$

be algebras with r-ary operations for each i in some indexed set I. Then, we have the algebra

$$\mathbf{A} \times \mathbf{B} = \langle A \times B, \star_i \rangle$$

where

$$\star_i((a_0, b_0), \ldots, (a_{r-1}, b_{r-1})) = (*_i(a_0, \ldots, a_{r-1}), \Box_i(b_0, \ldots, b_{r-1}))$$

with $a_j \in A$ and $b_j \in B$ for $0 \leq j \leq r-1$.

Problem 3

Prove that the congruence relations of $\mathbf{A}$ are exactly those subuniverses of $\mathbf{A} \times \mathbf{A}$ which happen to be equivalence relations on A.

Proof. ($\Rightarrow$) Let Θ be an equivalence relation on A. Define the algebra $\mathbf{T} = \langle T, \star_i \rangle$ for all $i \in I$ where

$$T = \{(a, a') \mid a, a' \in A, a \Theta a'\}$$

It is clear that $T \subseteq A \times A$ and defines an equivalence relation (since Θ is an equivalence relation). To see that it preserves $\star_i$, let $(a_0, a'_0), \ldots, (a_{r-1}, a'_{r-1}) \in T$. Then, for each $i \in I$

$$\star_i((a_0, a'_0), \ldots, (a_{r-1}, a'_{r-1})) = (*_i(a_0, \ldots, a_{r-1}), *_i(a'_0, \ldots, a'_{r-1}))$$

Now, since Θ is a congruence relation, we have that

$$*_i(a_0, \ldots, a_{r-1})\Theta *_i (a'_0, \ldots, a'_{r-1})$$

and so

$$(*_i(a_0, \ldots, a_{r-1}), *_i(a'_0, \ldots, a'_{r-1})) \in T$$

($\Leftarrow$) Let $\mathbf{E} = \langle E, \star_i \rangle$ for all $i \in I$ be an algebra where

$$E = \{(a, a') \mid a, a' \in A, a \text{ is equivalent to } a'\}$$

and so $\mathbf{E}$ is a subuniverse of $\mathbf{A} \times \mathbf{A}$. Define the relation Θ

$$a\Theta a' \text{ if and only if } (a, a') \in E.$$

It is clear that Θ is an equivalence relation (since E is an equivalence relation). To see that Θ preserves $\star_i$, suppose $a_0\Theta a'_0, \ldots, a_{r-1}\Theta a'_{r-1}$. Then, $(a_0, a'_0), \ldots, (a_{r-1}, a'_{r-1}) \in E$. Hence, for all $i \in I$

$$\star_i((a_0, a'_0), \ldots, (a_{r-1}, a'_{r-1})) = (*_i(a_0, \ldots, a_{r-1}), *_i(a'_0, \ldots, a'_{r-1}))$$

Since E is closed under $\star_i$, we have that

$$(*_i(a_0, \ldots, a_{r-1}), *_i(a'_0, \ldots, a'_{r-1})) \in E$$

and so

$$*_i(a_0, \ldots, a_{r-1})\Theta *_i (a'_0, \ldots, a'_{r-1})$$

□

Problem 4

Prove that the homomorphisms from $\mathbf{A}$ to $\mathbf{B}$ are exactly those subuniverses of $\mathbf{A} \times \mathbf{B}$ which are functions from A to B.

Proof. ($\Rightarrow$) Let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Define the algebra $\mathbf{H} = \langle H, \star_i \rangle$ for all $i \in I$ where

$$H = \{(a, h(a)) \mid a \in A\}$$

It is clear that $H \subseteq A \times B$ and defines a function from A to B (namely h). To see that it preserves $\star_i$, let $a_0, \ldots, a_{r-1} \in A$. Then, for each $i \in I$

$$\begin{aligned}
\star_i((a_0, h(a_0)), \ldots, (a_{r-1}, h(a_{r-1}))) &= (*_i(a_0, \ldots, a_{r-1}), \square_i(h(a_0), \ldots, h(a_{r-1}))) \\
&= (*_i(a_0, \ldots, a_{r-1}), h(\square_i(a_0, \ldots, a_{r-1}))) \\
&\in H
\end{aligned}$$

($\Leftarrow$) Let $\mathbf{F} = \langle F, \star_i \rangle$ for all $i \in I$ be an algebra where

$$F = \{(a, f(a)) \mid a \in A\}$$

for some function $f : A \to B$ (and so $\mathbf{F}$ is a subuniverse of $\mathbf{A} \times \mathbf{B}$). Since $\mathbf{F}$ is an algebra, we have for $a_0, \ldots, a_{r-1} \in A$ and for each $i \in I$

$$\star_i((a_0, f(a_0)), \ldots, (a_{r-1}, f(a_{r-1}))) = (*_i(a_0, \ldots, a_{r-1}), \square_i(f(a_0), \ldots, f(a_{r-1}))) \in F$$

and so

$$f(*_i(a_0, \ldots, a_{r-1})) = \square_i(f(a_0), \ldots, f(a_{r-1}))$$

In other words, f is a homomorphism. □

Problem 5

Prove that the projection functions associated with $\mathbf{A} \times \mathbf{B}$ are homomorphisms.

Proof. Define

$$\pi_0 : A \times B \to A$$
$$\pi_0(a, b) = a \text{ for all } a \in A \text{ and } b \in B$$

Now, let $a_0, \ldots, a_{r-1} \in A$ and $b_0, \ldots, b_{r-1} \in B$. Then, for each $i \in I$,

$$\begin{aligned}\pi_0(\star_i((a_0, b_0), \ldots, (a_{r-1}, b_{r-1}))) &= \pi_0((*_i(a_0, \ldots, a_{r-1}), \square_i(b_0, \ldots, b_{r-1}))) \\ &= *_i(a_0, \ldots, a_{r-1}) \\ &= *_i(\pi_0((a_0, b_0)), \ldots, \pi_0((a_{r-1}, b_{r-1})))\end{aligned}$$

Similarly, define

$$\pi_1 : A \times B \to B$$
$$\pi_1(a, b) = b \text{ for all } a \in A \text{ and } b \in B$$

Then, for all $i \in I$

$$\begin{aligned}\pi_1(\star_i((a_0, b_0), \ldots, (a_{r-1}, b_{r-1}))) &= \pi_1((*_i(a_0, \ldots, a_{r-1}), \square_i(b_0, \ldots, b_{r-1}))) \\ &= \square_i(b_0, \ldots, b_{r-1}) \\ &= \square_i(\pi_1((a_0, b_0)), \ldots, \pi_1((a_{r-1}, b_{r-1})))\end{aligned}$$

□

Problem 6

Derive a list of equations that follow from the equations axiomatizing the theory of groups.

Claim 1. *The distinguished element 1 in a group is the unique identity.*

Proof. Suppose that there exists another identity element $1'$. Then

$$1 = 1 \cdot 1' = 1'$$

□

Claim 2. *The element x^{-1} is the unique inverse of the element x.*

Proof. Suppose that x has another inverse x'. Then

$$x' = x' \cdot 1 = x' \cdot (xx^{-1}) = (x'x)x^{-1} = 1 \cdot x^{-1} = x^{-1}$$

□

Claim 3. $(xy)^{-1} = y^{-1}x^{-1}$

Proof. $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = xx^{-1} = 1$ □

Claim 4. $x^n x^k = x^{n+k}$

Proof. $x^n x^k = \underbrace{(x \cdots x)}_{\text{n times}} \underbrace{(x \cdots x)}_{\text{k times}} = \underbrace{x \cdots x}_{\text{n + k times}} = x^{n+k}$ □

Claim 5. $(x^n)^{-1} = (x^{-1})^n$

Proof.

$$\begin{aligned}
x^n(x^{-1})^n &= \underbrace{(x \cdots x)}_{\text{n times}} \underbrace{(x^{-1} \cdots x^{-1})}_{\text{n times}} \\
&= \underbrace{(x \cdots x)}_{\text{n-1 times}} (xx^{-1}) \underbrace{(x^{-1} \cdots x^{-1})}_{\text{n-1 times}} \\
&= \underbrace{(x \cdots x)}_{\text{n-1 times}} \cdot 1 \cdot \underbrace{(x^{-1} \cdots x^{-1})}_{\text{n-1 times}} \\
&= \underbrace{(x \cdots x)}_{\text{n-1 times}} \underbrace{(x^{-1} \cdots x^{-1})}_{\text{n-1 times}} \\
&= \cdots \\
&= xx^{-1} \\
&= 1
\end{aligned}$$

□

Problem 7

The five equations used to axiomatize groups are not all needed. Find a simpler set of equations that will serve.

We take only the following equations for our axiomatization of groups. For all elements x, y, z in the algebra $\mathbf{A} = \langle A, \cdot, {}^{-1}, 1 \rangle$

- $x(yz) = (xy)z$
- $xx^{-1} = 1$
- $x \cdot 1 = x$

From these, we derive the following.

Claim 6. $x^{-1}x = 1$

Proof.

$$\begin{aligned} x^{-1}x &= (x^{-1} \cdot 1)x \\ &= (x^{-1}(xx^{-1}))x \\ &= (x^{-1}x)(x^{-1}x) \\ (x^{-1}x)(x^{-1}x)^{-1} &= (x^{-1}x)(x^{-1}x)(x^{-1}x)^{-1} \\ 1 &= x^{-1}x \end{aligned}$$

□

Claim 7. $1 \cdot x = x$

Proof.

$$\begin{aligned} 1 \cdot x &= (xx^{-1})x \\ &= x(x^{-1}x) \\ &= x \cdot 1 \\ &= x \end{aligned}$$

□

Problem 8

State and prove a version of the isomorphism theorem from class that holds for algebraic systems generally, not just for groups.

Theorem 2. *(The Second Isomorphism Theorem) Let $\boldsymbol{A}$ be an algebra and let Θ and Φ be congruence relations on $\boldsymbol{A}$ such that $\Theta \subseteq \Phi$. Then ${}^{\Phi}\!/_{\Theta}$ is a congruence relation on ${}^{\boldsymbol{A}}\!/_{\Theta}$ and*

$$ {}^{\boldsymbol{A}}\!/_{\Theta}\!/_{\Phi/\Theta} \cong {}^{\boldsymbol{A}}\!/_{\Phi} $$

Proof. Define $h : {}^{\mathbf{A}}\!/_{\Theta} \to {}^{\mathbf{A}}\!/_{\Phi}$ by

$$ h({}^{a}\!/_{\Theta}) = {}^{a}\!/_{\Phi} \text{ for all } a \in \mathbf{A} $$

Claim 8. *h is well-defined.*

Proof. Suppose ${}^{a}\!/_{\Theta} = {}^{b}\!/_{\Theta}$. Then $(a, b) \in \Theta \subseteq \Phi$, and so ${}^{a}\!/_{\Phi} = {}^{b}\!/_{\Phi}$. □

Claim 9. *h is onto ${}^{\boldsymbol{A}}\!/_{\Phi}$.*

Proof. Let ${}^{a}\!/_{\Phi} \in {}^{\mathbf{A}}\!/_{\Phi}$. We see that $h({}^{a}\!/_{\Theta}) = {}^{a}\!/_{\Phi}$. □

Claim 10. *h is a homomorphism.*

Proof.

$$ \begin{aligned} h({}^{a}\!/_{\Theta} \cdot {}^{b}\!/_{\Theta}) &= h({}^{ab}\!/_{\Theta}) \\ &= {}^{ab}\!/_{\Phi} \\ &= {}^{a}\!/_{\Phi} \cdot {}^{b}\!/_{\Phi} \\ &= h({}^{a}\!/_{\Theta}) \cdot h({}^{b}\!/_{\Theta}) \end{aligned} $$

□

Claim 11. $Ker(h) = {}^{\Phi}\!/_{\Theta}$

Proof.

$$ \begin{aligned} ({}^{a}\!/_{\Theta}, {}^{b}\!/_{\Theta}) \in Ker(h) &\Leftrightarrow h({}^{a}\!/_{\Theta}) = h({}^{b}\!/_{\Theta}) \\ &\Leftrightarrow {}^{a}\!/_{\Phi} = {}^{b}\!/_{\Phi} \\ &\Leftrightarrow (a, b) \in \Phi \end{aligned} $$

Hence

$$\begin{aligned} Ker(h) &= \{(a/\Theta, b/\Theta) \mid (a,b) \in \Phi\} \\ &= \Phi/\Theta \end{aligned}$$

□

Now, by the Homomorphism Theorem, there is an isomorphism between $\mathbf{A}/\Theta/\Phi/\Theta$ and $\mathbf{A}/\Phi$, that is $\mathbf{A}/\Theta/\Phi/\Theta \cong \mathbf{A}/\Phi$. □

Problem 10

Let $\mathbf{G}$ be a group. Prove that $\mathbf{G}$ cannot have four distinct proper normal subgroups $\mathbf{N}_0, \mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3$ so that $\mathbf{N}_0 \leq \mathbf{N}_1 \leq \mathbf{N}_2 \leq \mathbf{G}$ and so that $N_1 N_3 = G$ and $N_2 \cap N_3 = N_0$.

Proof. Suppose we have normal subgroups of the desired form. Let $n_2 \in N_2 \subset G$. Then, $n_2 = n_1 n_3$ for some $n_1 \in N_1$ and $n_3 \in N_3$ (since $N_1 N_3 = G$). We have that $n_3 = n_1^{-1} n_2 \in N_2$ (since $n_1^{-1} \in N_1 \subset N_2$). Hence, $n_3 \in N_2 \cap N_3 = N_0 \subset N_1$. Since $n_3 \in N_1$, we have that $n_2 = n_1 n_3 \in N_1$. Therefore, $N_2 \subset N_1$, which implies that $N_1 = N_2$. This is a contradiction with the fact that N_1 and N_2 are distint. □

Problem 11

Let $\mathbf{H}$ and $\mathbf{K}$ be subgroups of the group $\mathbf{G}$ each of finite index in $\mathbf{G}$. Prove that $\mathbf{H} \cap \mathbf{K}$ is also a subgroup of finite index in $\mathbf{G}$.

Claim 12. *$H \cap K$ is a subset of G.*

Proof. Let $a \in H \cap K$. Then, $a \in H$. Since $\mathbf{H}$ is a subgroup of G, we have that $a \in G$. □

Claim 13. ***$H \cap K$** contains the identity.*

Proof. $\mathbf{H}$ and $\mathbf{K}$ are both groups, so we have $1 \in H$ and $1 \in K$. Therefore, $1 \in H \cap K$. □

Claim 14. ***$H \cap K$** is closed under the taking of inverses.*

Proof. Let $a \in H \cap K$. Then, $a \in H$ and $a \in K$. Since $\mathbf{H}$ and $\mathbf{K}$ are both groups, we have that $a^{-1} \in H$ and $a^{-1} \in K$. Therefore, $a^{-1} \in H \cap K$. □

Claim 15. ***$H \cap K$** is closed under addition.*

Proof. Let $a, b \in H \cap K$. Then, a, b belong to both H and K. Since $\mathbf{H}$ and $\mathbf{K}$ are both groups, we have that $a + b$ belongs to both H and K. Therefore, $a + b \in H \cap K$. □

By the previous claims, we see that $\mathbf{H} \cap \mathbf{K}$ is a subgroup of $\mathbf{G}$.

Claim 16. *$\boldsymbol{H} \cap \boldsymbol{K}$ has finite index in $\boldsymbol{G}$.*

Proof. Define the function

$$f : {}^{G}\!/_{H \cap K} \to {}^{G}\!/_{H} \times {}^{G}\!/_{K}$$
$$f(a(H \cap K)) = (aH, aK) \text{ for all } a \in G$$

To see that this function is well-defined, suppose $a(H \cap K) = b(H \cap K)$. Then, a and b belong to the same equivalence class in ${}^{G}\!/_{H \cap K}$. We see that

$$\begin{aligned} & a(H \cap K) \subseteq aH \\ \Rightarrow & b(H \cap K) \subseteq aH \\ \Rightarrow & aH = bH \end{aligned}$$

and similarly

$$\begin{aligned} & a(H \cap K) \subseteq aK \\ \Rightarrow & b(H \cap K) \subseteq aK \\ \Rightarrow & aK = bK \end{aligned}$$

Hence, $(aH, aK) = (bH, bK)$, and so f is well-defined.

We claim that this function is one-to-one. Suppose $(aH, aK) = (bH, bK)$. Then $aH = bH$ and $aK = bK$, which implies that a and b belong to the same equivalence class in ${}^{G}\!/_{H}$ as well as the same equivalence class in ${}^{G}\!/_{K}$. Therefore, a and b belong to the same equivalence class in ${}^{G}\!/_{H \cap K}$. That is, $a(H \cap K) = b(H \cap K)$.

Now, f is a one-to-one map sending each coset of ${}^{G}\!/_{H \cap K}$ into a finite range (since each of H and K have finite index in G), so it must be that the domain is finite. That is, $H \cap K$ has finite index in G. □

Problem 12

Prove that there is no group $\mathbf{G}$ such that ${}^{\mathbf{G}}\!/_{\mathbf{Z(G)}} \cong \mathbb{Z}$, where $\mathbb{Z}$ denotes the group of integers under addition.

Proof. Suppose ${}^{G}\!/_{Z(G)} \cong \mathbb{Z}$ for some group G. Since $\mathbb{Z}$ is cyclic, ${}^{G}\!/_{Z(G)}$ is cyclic. Let $aZ(G)$ generate ${}^{G}\!/_{Z(G)}$. Then, every coset is of the form $a^n Z(G)$ for some integer n. Since

the cosets partition G, we have that every element of G is of the form $a^n c$ for some integer n and some element $c \in Z(G)$. Let g_1, g_2 be arbitrary elements of G with $g_1 = a^{n_1}c_1$ and $g_2 = a^{n_2}c_2$. It follows that

$$\begin{aligned} g_1 g_2 &= a^{n_1}c_1 a^{n_2}c_2 \\ &= a^{n_2}c_2 a^{n_1}c_1 \qquad \text{(since } c_1, c_2 \in Z(G) \text{ and powers of } a \text{ commute)} \\ &= g_2 g_1 \end{aligned}$$

Hence, any two elements of G commute. That is, $Z(G) = G$, and so $G/Z(G) = \{1\}$, which contradicts our assumption that $G/Z(G) \cong \mathbb{Z}$. □

Problem 13

Let p be the smallest prime that divides the cardinality of the finite group G. Prove that any subgroup of G of index p must be normal.

Proof. Let H be a subgroup of G having index p in G. Let π_H be the action of left multiplication by G on the cosets of H in G. Since pi_H is a homomorphism, $ker(\pi_H)$ is normal in G and $[G : K] = [G : H][H : ker(\pi_H)]$. Now, since H has p left cosets, $G/ker(\pi_H)$ is isomorphic to some subgroup of of SYM_p. By Lagrange's theorem, we have that $|G/ker(\pi_H)| = p[H : ker(\pi_H)]$ divides $p!$. That is, $[H : ker(\pi_H)]$ divides $\frac{p!}{p} = (p-1)!$. The minimality of p implies that $[H : ker(\pi_H)] = 1$, and so $ker(\pi_H) = H$. Therefore, H is normal in G. □

Problem 14

How many elements of order 7 are there in a simple group of order 168?

Proof. Note first that $168 = 2^3 * 3 * 7$. By Sylow's theorem, we have that $|Syl^7(G)| \equiv 1 \pmod 7$ and $|Syl^7(G)| \mid 24$. So, $|Syl^7(G)|$ is equal to 1 or 8. Since G is simple, it cannot be that $|Syl^7(G)| = 1$, as this would imply that G has a unique (and so normal) Sylow 7-subgroup. Now, all elements of order 7 appear in a Sylow 7-subgroup. Furthermore, the 8 Sylow 7-subgroups are disjoint except for the identity element. Therefore, there are $8 * 6 = 48$ elements of order 7. □

Problem 15

Let N be a normal subgroup of the finite group G and let K be a Sylow p-subgroup of N for some prime p. Prove that $G = N_G(K)N$.

Proof. Let g be an element of G. Since K is a Sylow p-subgroup of the normal subgroup N, we have that gKg^{-1} is also a Sylow p-subgroup of N. By Sylow's theorem, all Sylow p-subgroups are conjugate, so we can find an element n of N so that $ngKg^{-1}n^{-1} = K$. The lefthand side can be rewritten as $(ng)K(ng)^{-1}$, and so we see that ng is an element of $N_G(K)$. That is, $g = n^{-1}(ng) \in NN_G(K)$. Since N is normal in G, $NN_G(K) = N_G(K)N$, and so we have shown that $g \in N_G(K)N$.

The reverse inclusion is easy, since $N_G(K) \leq G$ and $N \leq G$. Therefore, $G = N_G(K)N$. □

Problem 16

Prove that there is no simple group G of order 56.

Proof. Note first that $56 = 2^3 * 7$. By Sylow's theorem, we have that $|Syl^7(G)| \equiv 1 \pmod 7$ and $|Syl^7(G)| \mid 8$. So, $|Syl^7(G)|$ is equal to 1 or 8. If $|Syl^7(G)| = 1$, then G has a unique (and so normal) Sylow 7-subgroup. If $|Syl^7(G)| = 8$, then there are $8 * 6 = 48$ elements of order 7, leaving 8 elements which comprise a unique (and so normal) Sylow 2-subgroup. In either case, we see that G contains a normal subgroup, and so we see that G cannot be normal. □

Problem 17

Prove that if $\mathbf{G}$, $\mathbf{H}$, and $\mathbf{K}$ are finite Abelian groups and $\mathbf{G} \times \mathbf{H} \cong \mathbf{G} \times \mathbf{K}$, then $\mathbf{H} \cong \mathbf{K}$.

Proof. Since $\mathbf{G}$, $\mathbf{H}$, and $\mathbf{K}$ are finite Abelian groups, they are each isomorphic to some direct product of cyclic groups of prime power order.

Observe that, since $\mathbf{G} \times \mathbf{H} \cong \mathbf{G} \times \mathbf{K}$ and all the groups are finite,

$$|\mathbf{G}||\mathbf{H}| = |\mathbf{G} \times \mathbf{H}| = |\mathbf{G} \times \mathbf{K}| = |\mathbf{G}||\mathbf{K}|$$

Hence, $|\mathbf{H}| = |\mathbf{K}|$.

Now, suppose for the sake of contradiction that $\mathbf{H}$ is not isomorphic to $\mathbf{K}$. Since they are of the same finite order, it must be that one of the cyclic groups comprising $\mathbf{H}$ appears with different multiplicity than in $\mathbf{K}$ (note one of these multiplicites may be 0). Let the order of this cyclic factor be p^k for some prime p. We see that $\mathbf{H}$ and $\mathbf{K}$ necessarily have differing numbers of elements of order p^k. This implies that $\mathbf{G} \times \mathbf{H}$ and $\mathbf{G} \times \mathbf{K}$ do not have the same number of elements of order p^k, and so are not isomorphic, which is a contradiction. Therefore, it must be that $\mathbf{H} \cong \mathbf{K}$. □

Problem 18

Prove that every group of order 35 is cyclic.

Proof. Observe first that $35 = 5 \cdot 7$. Consider the Sylow p-subgroups of G. Sylow's theorem gives

- $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 7$, so $n_5 = 1$
- $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 5$, so $n_7 = 1$

Hence, $\mathbf{G}$ has a unique Sylow 5-subgroup $\mathbf{N}_5$ and a unique Sylow 7-subgroup $\mathbf{N}_7$. The uniqueness of each of these groups implies that they are normal in $\mathbf{G}$.

Observe next that $\mathbf{N}_5 \cap \mathbf{N}_7$ is trivial, since only the identity element can have order dividing both $|\mathbf{N}_5|$ and $|\mathbf{N}_7|$. By the Third Isomorphism theorem, we have

$$\mathbf{N}_5\mathbf{N}_7 \big/ \mathbf{N}_7 \cong \mathbf{N}_5 \big/ \mathbf{N}_5 \cap \mathbf{N}_7 = \mathbf{N}_5$$

Applying Lagrange's theorem, we have

$$\begin{aligned} \left|\mathbf{N}_5\mathbf{N}_7 \big/ \mathbf{N}_7\right| &= |\mathbf{N}_5| \\ \frac{|\mathbf{N}_5\mathbf{N}_7|}{|\mathbf{N}_7|} &= |\mathbf{N}_5| \\ |\mathbf{N}_5\mathbf{N}_7| &= |\mathbf{N}_5||\mathbf{N}_7| = |\mathbf{G}| \end{aligned}$$

Hence, $\mathbf{G} \cong \mathbf{N}_5 \times \mathbf{N}_7$.

Now, both of $\mathbf{N}_5$ and $\mathbf{N}_7$ are cyclic (and so Abelian), since they are of prime order. We claim that $\mathbf{G}$ is also Abelian. Let (a_1, b_1) and (a_2, b_2) be elements of $\mathbf{G}$. It follows that

$$\begin{aligned} (a_1, b_1) * (a_2, b_2) &= (a_1a_2, b_1b_2) \\ &= (a_2a_1, b_2b_1) \\ &= (a_2, b_2)(a_1, b_1) \end{aligned}$$

Hence, $\mathbf{G}$ is Abelian. We see that $\mathbf{G}$ is a finite Abelian group with k^2 not dividing its order for all $k > 1$. By problem 20, we conclude that $\mathbf{G}$ is cyclic. $\square$

Problem 19

Describe, up to isomorphism, all groups of order 1225.

Proof. Observe first that $1225 = 5^2 7^2$. Consider the Sylow p-subgroups of G. Sylow's theorem gives

- $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 49$, so $n_5 = 1$
- $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 25$, so $n_7 = 1$

Hence, $\mathbf{G}$ has a unique Sylow 5-subgroup $\mathbf{N}_5$ and a unique Sylow 7-subgroup $\mathbf{N}_7$. The uniqueness of each of these groups implies that they are normal in $\mathbf{G}$.

Observe next that $\mathbf{N}_5 \cap \mathbf{N}_7$ is trivial, since only the identity element can have order dividing both $|\mathbf{N}_5|$ and $|\mathbf{N}_7|$. By the Third Isomorphism theorem, we have

$$\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7 \cong \mathbf{N}_5/\mathbf{N}_5 \cap \mathbf{N}_7 = \mathbf{N}_5$$

Applying Lagrange's theorem, we have

$$\begin{aligned} \left|\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7\right| &= |\mathbf{N}_5| \\ \frac{|\mathbf{N}_5\mathbf{N}_7|}{|\mathbf{N}_7|} &= |\mathbf{N}_5| \\ |\mathbf{N}_5\mathbf{N}_7| &= |\mathbf{N}_5||\mathbf{N}_7| = |\mathbf{G}| \end{aligned}$$

Hence, $\mathbf{G} \cong \mathbf{N}_5 \times \mathbf{N}_7$.

We proceed by showing $\mathbf{N}_5$ is Abelian. Since $\mathbf{N}_5$ is of prime power order, it has a nontrivial center $Z(\mathbf{N}_5)$. Furthermore, $Z(\mathbf{N}_5)$ is normal in $\mathbf{N}_5$, so $\mathbf{N}_5/Z(\mathbf{N}_5)$ is a group of size 1 or 5. If it is of size 5, then it is cyclic. We claim that this is impossible in general.

Claim 17. *If a group $\boldsymbol{G}$ properly contains its center, then $\boldsymbol{G}/Z(\boldsymbol{G})$ is not cyclic.*

Proof. Suppose, to the contrary, that $\mathbf{G}/Z(\mathbf{G})$ is cyclic generated by $aZ(\mathbf{G})$. We argue that G is Abelian. Let b and c be elements of G. We can find integers m and n so that

$$\begin{aligned} bZ(\mathbf{G}) &= a^m Z(\mathbf{G}) \\ cZ(\mathbf{G}) &= a^n Z(\mathbf{G}) \end{aligned}$$

This further implies that we can find elements d and e in $Z(\mathbf{G})$ so that

$$\begin{aligned} b &= a^m d \\ c &= a^n e \end{aligned}$$

Observe that d and e commute freely with any element since they are in the center. Furthermore, powers of a commute with each other. It follows that

$$\begin{aligned} bc &= (a^m d)(a^n e) \\ &= (a^n e)(a^m d) \\ &= cb \end{aligned}$$

Hence, $\mathbf{G}$ is Abelian, so $Z(\mathbf{G}) = \mathbf{G}$, which contradicts our assumption that $\mathbf{G}$ properly contains its center. Therefore, we conclude that $\mathbf{G}/Z(\mathbf{G})$ is not cyclic. □

Citing the claim above, we conclude that $\mathbf{N}_5/Z(\mathbf{N}_5)$ is of size 1. In other words, $\mathbf{N}_5$ is Abelian.

Similarly, we can show that $\mathbf{N}_7$ is Abelian (replace every occurrence of "5" with "7" in the argument for $\mathbf{N}_5$).

Applying the Fundamental Theorem of Finite Abelian Groups, we conclude that $\mathbf{G}$ is isomorphic to one of

$$\mathbb{Z}_{49} \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_{49} \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{25} \times \mathbb{Z}_7 \times \mathbb{Z}_7$$
$$\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

□

Problem 20

Let $\mathbf{G}$ be a finite Abelian group. Prove that if $|\mathbf{G}|$ is not divisible by k^2 for any $k > 1$, then $\mathbf{G}$ is cyclic.

Proof. By the Fundamental Theorem of Finite Abelian Groups, $\mathbf{G}$ has a unique decomposition as a direct product of cyclic groups of prime power order. More precisely,

$$\mathbf{G} \cong \mathbb{Z}_{{p_1}^{n_1}} \times \cdots \times \mathbb{Z}_{{p_k}^{n_k}}$$

where each p_i is a prime number and each $n_i \geq 1$. Since k^2 does not divide the order of $\mathbf{G}$ for any $k > 1$, it must be that $n_i = 1$ for all i (otherwise, p_i^2 divides the order of $\mathbf{G}$ for some i). We have now

$$\mathbf{G} \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$$

We see that $|\mathbf{G}| = p_1 \cdots p_k$. We claim that $\mathbf{G}$ has an element of order $p_1 \cdots p_k$, and hence is cyclic.

Consider the element $\underbrace{(1, \ldots, 1)}_{\text{k times}}$ of $\mathbf{G}$. We see that $(1, \cdots, 1)^m = (0, \cdots, 0)$ if and only if m is the least common multiple of $p_1, \cdots, p_k$. Since the p_i are prime (and so relatively prime), $m = p_1 \cdots p_k$. That is, $(1, \cdots, 1)$ has order $p_1 \cdots p_k$, and so $\mathbf{G}$ is cyclic. □

Problem 21.

Prove that $\mathrm{Aut}(S_n) \cong S_n$ for every natural number n.

Proof. Let $\sigma \in S_n$ and define $f(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in S_n$. We claim that f is an automorphism of S_n: for all $\tau, \delta \in S_n$ we have $f(\tau\delta) = \sigma\tau\delta\sigma^{-1} = (\sigma\tau\sigma^{-1})(\sigma\delta\sigma^{-1}) = f(\tau)f(\delta)$. So f is a homomorphism. Now, $f(\tau) = f(\delta) \Leftrightarrow \sigma\tau\sigma^{-1} = \sigma\delta\sigma^{-1} \Leftrightarrow \tau = \delta$ so f is one-to-one. Also, for all $\tau \in S_n$, there exists $\sigma^{-1}\tau\sigma \in S_n$, such that $f(\sigma^{-1}\tau\sigma) = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1} = \tau$. So, f is onto. Hence, f is an isomorphism from S_n to S_n; i.e. $f \in \mathrm{Aut}(S_n)$

Now, let $\Phi : S_n \to \mathrm{Aut}(S_n)$. By using $\Phi_\sigma = f$ to denote $\Phi(\sigma) = f$, we have $\Phi_\sigma(\tau) = \sigma\tau\sigma^{-1}$ for all $\tau \in S_n$. Also, Φ is a homomorphism: Let $\tau \in S_n$. Then for all $\sigma, \delta \in S_n$, we have $\Phi_{\sigma\delta}(\tau) = (\sigma\delta)\tau(\sigma\delta)^{-1} = \sigma\delta\tau\delta^{-1}\sigma^{-1} = \sigma\Phi_\delta(\tau)\sigma^{-1} = \Phi_\sigma(\Phi_\delta(\tau)) = \Phi_\sigma \circ \Phi_\delta(\tau)$.

Claim: Φ is one-to-one.

$$\begin{aligned} & \sigma \in \ker \Phi \\ \Leftrightarrow \quad & \Phi_\sigma = \mathrm{Id}_{S_n} \\ \Leftrightarrow \quad & \Phi_\sigma(\tau) = \mathrm{Id}(\tau) \ \ \forall \tau \in S_n \\ \Leftrightarrow \quad & \sigma\tau\sigma^{-1} = \tau \ \ \forall \tau \in S_n \\ \Leftrightarrow \quad & \sigma\tau = \tau\sigma \ \ \forall \tau \in S_n \end{aligned}$$

Since S_n is the group of permutations, the identity is the only element in S_n that commutes with every element in S_n. So, $\ker \Phi = \{1\}$. Therefore, Φ is one-to-one. Since both S_n and $\mathrm{Aut}(S_n)$ are finite, it follows from Φ begin one-to-one that Φ is onto. Thus Φ is an isomorphism. It follows that $\mathrm{Aut}(S_n) \cong S_n$. □

Problem 22.
Let p be a prime number. Prove that if a and b are elements of the symmetric group S_p, where a has order p and b is a transposition, then $\{a, b\}$ generates S_p.

Proof. Let $a, b \in S_p$ and let b be a transposition. Without loss of generality, let $b = (0\ 1)$. As a has order p and p is prime p, we have that a is p-cycle. Therefore, $a^k = (0\ 1 \ldots)$ for some k. We can re-index the other elements so that we have $a^k = (0\ 1 \ldots p-1)$. Let $c = a^k$. Then $cbc^{-1} = (0\ 1 \ldots p-1)(0\ 1)(p-1 \ldots 0\ 1) = (0)(1\ 2)(3)...(p-1) = (1\ 2)$. By induction, we have $c^k b c^{-k} = c(c^{k-1}bc^{-k+1})c^{-1} = (k+1\ \ k+2)$. Therefore, we have that $(0\ 1), (1\ 2), ..., (p-2\ \ p-1)$ are generated by $\{a, b\}$. Let (xy) be a transposition. Then $(x\ \ x+1)(x+1\ \ x+2)\cdots(y-1\ \ y) = (x\ \ y)$ and $(x\ \ y)$ is also generated by $\{a, b\}$. As every permutation can be decomposed into transpositions we conclude that $\{a, b\}$ generates S_p. □

Problem 23.
Let $H \leq G$. Prove that $N_G(H)/C_G(H)$ is embeddable into $\mathrm{Aut}(H)$.

Proof. We begin by recalling the definitions of $N_G(H)$ and $C_G(H)$.

$$\begin{aligned} N_G(H) &= \{g \in G \mid gH = Hg\} \\ &= \{g \in G \mid H = gHg^{-1}\} \end{aligned}$$

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

Now, define a map $h : N_G(H) \to \mathrm{Aut}(H)$ by $h(n) = \varphi_n$ for each $n \in N_G(H)$, where we have $\varphi_n(h) = nhn^{-1}$ for $h \in H$. Since φ_n acts on H by conjugation, we see that $\varphi_n \in \mathrm{Aut}(H)$.
Claim: $h : N_G(H) \to \mathrm{Aut}(H)$ is a homomorphism. Let $a, b \in N_G(H)$. We have

$$\begin{aligned} h(ab) &= \varphi_{ab} \\ &= \varphi_a\varphi_b \\ &= h(a)h(b) \end{aligned}$$

Claim: $\ker h = C_G(H)$. We have

$$\begin{aligned} \ker h &= \{n \mid \varphi_n(h) = h \text{ for all } h \in H\} \\ &= \{n \mid nhn^{-1} = h \text{ for all } h \in H\} \\ &= C_G(H) \end{aligned}$$

By the isomorphism theorems, we now have $N_G(H)/C_G(H) \cong \mathrm{im}\, h \leq \mathrm{Aut}(H)$ which is what we wanted to establish. □

Problem 24.
Let G be a group of order n. Define $\varphi : G \to G$ by $\varphi(a) = a^{n^2+3n+1}$ for all $a \in G$. Prove that φ is an automorphism of G.

Proof. First, we show that $a^n = 1$, for all $a \in G$. Let $a \in G$ and $|\langle a \rangle| = m$. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$, i.e. $m \mid n$. Let $n = mq$ for some $q \in \mathbb{N}$. Then $a^n = a^{mq} = (a^m)^q = 1$. Now, $\varphi(a) = a^{n^2+3n+1} = a^{n^2+3n} \cdot a = (a^n)^{n+3} \cdot a = 1 \cdot a = a$, for all $a \in G$. Therefore, φ is the identity map from G to G. So, φ is an automorphism of G. □

Problem 25.
(1) Let I and J be ideals of a commutative ring $\mathbf{R}$ with $I + J = R$. Prove that $IJ = I \cap J$.
(2) Let I, J, and K be ideals of a principal ideal domain. Prove that $I \cap (J + K) = I \cap J + I \cap K$

Proof. 1) Let $x \in IJ$. Then $x = x_i + x_j$ where $x_i \in I$ and $x_j \in J$. Therefore, since I and J are ideals, by definition, $x_i x_j \in I$ and $x_i x_j \in J$. Thus, $IJ \subseteq I \cap J$.
Let $x \in I \cap J$. Since $I + J = R$, then $1 = i + j$ where $i \in I$ and $j \in J$. Then $x = 1x = (i + j)x = ix + jx$ and therefore, $x \in IJ$. So, $I \cap J \subseteq IJ$ and $IJ = I \cap J$. □

Problem 26.
Let R be a commutative ring and I be a proper prime ideal of R such that R/I satisfies the descending chain condition on ideals. Prove that R/I is a field.

Proof. Since I is a proper prime ideal of R, R/I is an integral domain. Now, pick $a \in R/I$ with $a \neq 0$, and consider the ideal generated by a. Since R/I satisfies the descending chain condition, we have

$$(a) \supseteq (a^2) \supseteq (a^3) \supset \cdots \supset (a^k) = (a^{k+1}) = \cdots$$

So we have $a^k = ba^{k+1}$ for some b. Now, since R/I is an integral domain, we see that $ba^{k+1} - a^k = 0$ and so $ba = 1$. Thus $b = a^{-1}$, and so R/I is a field. □

Problem 27.
Let $\mathbf{R}$ be a commutative ring and I be an ideal which is contained in a prime ideal P. Prove that the collection of prime ideals contained in P and containing I has a minimal member.

Proof. Let F be the set of all prime ideals that contain I and are contained in P. Let C be chain of prime ideals in F ordered by $\supseteq$. Observe that $\cap C$ is an upper bound. Furthermore, $I \subseteq \cap C \subseteq P$. We claim that $\cap C$ is indeed a prime ideal of $\mathbf{R}$.

We see that 0 is an element of every prime ideal in the chain, so 0 is an element of $\cap C$.

Let a and b be elements of $\cap C$. We have that a and b belong to every prime ideal in the chain, so $a + b$ and $-a$ belong to every prime ideal in the chain. Hence, $a + b$ and $-a$ belong to $\cap C$.

Let a be an element of $\cap C$ and r an element of the ring $\mathbf{R}$. We see that a belongs to every prime ideal in the chain, so ra and ar belong to every prime ideal in the chain. Hence, ra and ar belong to $\cap C$.

Let ab be an element of $\cap C$. We see that ab belongs to every prime ideal in the chain. Hence, either a or b (or both) belongs to every prime ideal in the chain. Since the chain is ordered by $\supseteq$, every prime ideal contains a or every prime ideal contains b (or both). In other words, we cannot have prime ideals P_i and P_j with $P_i \supseteq P_j$, $a \in P_i \not\ni b$, and $a \notin P_j \ni b$. Hence, either a or b (or both) belongs to $\cap C$.

The preceeding observations imply that $\cap C$ is indeed a prime ideal of $\mathbf{R}$. By Zorn's Lemma, we conclude that F has a minimal element (i.e. a maximal element with respect to $\supseteq$). □

Problem 28.
Let X be a finite set and let $\mathbf{R}$ be the ring of functions from X into the field $\mathbb{R}$ of real numbers. Prove that an ideal M of $\mathbf{R}$ is maximal if and only if there is an element $a \in X$ such that $M = \{f \mid f \in R \text{ and } f(a) = 0\}$.

Proof. To prove the first direction, let $X = \{x_1, x_2, \ldots, x_n\}$, $R = \{f \mid f : X \to \mathbb{R}\}$. Without of loss of generality, let $a = x_1 \in X$, let $M = \{f \mid f \in R \text{ and } f(x_1) = 0\}$. Now, we show that M is a maximal ideal. Clearly, M is a proper ideal of R. Let I be an ideal of R such that $M \subseteq I$ and $M \neq I$. Then there exists $f_1 \in I$, $f_1 \notin M$. So, $f_1(x_1) \neq 0$. Now, define f_i for $2 \leq i \leq n$, $1 \leq j \leq n$ by

$$f_i(x_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

Then, $f_i(x_1) = 0$ for $i = 2, \ldots, n$. So, $f_i(x) \in M \subseteq I$ for $i = 2, \ldots, n$. Now, let

$$h(x) := \frac{f_1(x)}{f_1(x_1)} + f_2(x) + \cdots + f_n(x) \in I$$

Notice that $h(x) = 1$ for all $x_i \in X$. Therefore $I = R$. This means that M is an maximal ideal of R.
To prove the other direction, Let M be a maximal ideal of R. Assume that for all $x_i \in X$, there exists $g_i \in M$, such that $g_i(x_i) \neq 0$. Now, define $h_i(x)$ for $i = 1, \ldots, n$ and $j = 1, \ldots, n$ by

$$h_i(x_j) = \begin{cases} \frac{1}{g_i(x_i)} & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

Then, $h_i(x)g_i(x) \in M$ for $i = 1, \ldots, n$. Let

$$\phi(x) := h_1(x)g_1(x) + h_2(x)g_2(x) + \cdots + h_n(x)g_n(x) \in M.$$

Also, notice that $\phi(x) \equiv 1$. This means that $M = R$. This is a contradiction. Therefore our assumption must be false. So $M \subseteq \{f \mid f \in R \text{ and } f(a) = 0\}$ for some $a \in X$. Since we already showed that the right set is a maximal ideal. So, $M = \{f \mid f \in R \text{ and } f(a) = 0\}$. □

Problem 29.
Let $\mathbf{R}$ be a commutative ring and let n be a positive integer. Let $J, I_0, I_1, \ldots, I_{n-1}$ be ideals of $\mathbf{R}$ so that I_k is a prime ideal for every $k < n$ and so that $J \subseteq I_0 \cup \cdots \cup I_{n-1}$. Prove that $J \subseteq I_k$ for some $k < n$.

Proof. When $n = 1$, the claim is trivial. Suppose it holds for $n = k$. That is, if J is contained in a the union of k prime ideals, then J is contained in one of them. Now, for $n = k + 1$, $J \subseteq I_0 \cup \cdots I_k$. Suppose that each I_i is necessary. That is, for each i, we can find $a_i \in J$ with the property that $a_i \in I_i$ but $a_i \notin \bigcup_{j \neq i} I_j$. If this were not the case (that

is, no such element exists for some I_i) then $J \subseteq I_0 \cup \cdots \cup I_{i-1} \cup I_{i+1} \cup \cdots \cup I_k$, and we are done after an appeal to the inductive hypothesis. Now, consider the sum $\sum_j \prod_{i \neq j} a_i$. This sum belongs to J (since J is an ideal), so it must belong to the union of the prime ideals. Hence, it belongs to at least one of the prime ideals. Without loss of generality, suppose it is I_0. Since $a_0 \in I_0$ and I_0 is an ideal, all terms containing a_0 belong to I_0. By subtraction, we conclude that $a_1 \cdots a_k \in I_0$. Since I_0 is prime, we have that one of the a_i belongs to I_0, which is a contradiction. Therefore, it must be that one of the I_i is not necessary, and so J is contained in the union of k prime ideals. By the inductive hypothesis, we conclude that J is contained in one of these ideas. □

Problem 30.
Let $\mathbf{R}$ be a nontrivial commutative ring and let J be the intersection of all the maximal proper ideals of $\mathbf{R}$. Prove that $1 + a$ is a unit of $\mathbf{R}$ for all $a \in J$.

Proof. Let $a \in J$. Then $a \in M$ for each M. Since each M is a proper maximal ideal, we have $1 \notin M$, and in particular, $1+a \notin M$. As each M is maximal, R/M is a field. Since $1+a \notin M$, we see that $1 + a + M \neq 0 + M$. Now, R/M is a field, so there exists $b_M + M \in R/M$ such that $(1+a+M)(b_M+M) = 1+M$. Then $(1+a)b_M+M = 1+M \Rightarrow (1+a)b_M-1 \in 0+M$; in other words, $(1 + a)$ is a unit of R. □

Problem 31.
Let $\mathbf{F}$ be a field and let $p(x) \in \mathbf{F}[x]$ be a polynomial of degree n. Prove that $p(x)$ has at most n distinct roots in $\mathbf{F}$.

Proof. We proceed by induction on the degree n. Base step: if $n = 1$, then let $p(x) = ax+b$ for some $a, b \in \mathbf{F}$, $a \neq 0$. Let $p(x) = 0$, we have $ax = -b$. Since $\mathbf{F}$ is a field, we can multiply both sides of the equation by the inverse of a. It follows that $x = -\frac{b}{a} \in \mathbf{F}$ is a root of $p(x)$. Induction step: Assume $p(x)$ has at most n roots for $n \leq m$. Now, consider $n = m + 1$, let $c \in \mathbf{F}$ such that $p(c) = 0$. Then, by the factor theorem, $p(x) = q(x)(x - c)$ for some $q(x) \in \mathbf{F}[x]$ with $\deg q(x) \leq m$. By the induction hypothesis, $q(x)$ has at most m distinct roots. Therefore, $p(x)$ has at most $m + 1 = n$ distinct roots. □

Problem 32. Let $\mathbf{F}$ be a field and let $\mathbf{F}^*$ be its (multiplicative) group of nonzero elements. Let $\mathbf{G}$ be any finite subgroup of $\mathbf{F}^*$. Prove that $\mathbf{G}$ must be cyclic.

Proof. As $\mathbf{G}$ is a finite abelian group, the fundamental theorem of finite abelian groups gives us

$$\mathbf{G} \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}$$

where each d_i is a prime power. Let $m = \text{lcm}[d_1, d_2, \ldots, d_r]$ and note that $m \leq d_1 d_1 \cdots d_r$. For each $a_i \in C_{d_i}$ we have $a_i^m = 1$ since $a_i^{d_i} = 1$ in C_{d_i} and $d_i \mid m$. Thus for all $a \in \mathbf{G}$ we have $a^m = 1$, and so every element of $\mathbf{G}$ is a zero of the polynomial $x^m - 1$. By a previous homework problem, we know that $x^m - 1$ has at most m zeros in $\mathbf{F}$. Since $a^m - 1 = 0$ for all elements of $\mathbf{G}$ we must have $m \geq d_1 d_2 \cdots d_r$. Hence $m = d_1 d_2 \cdots d_r$. Therefore the primes in the prime powers d_i are distinct, and we see that $\mathbf{G} \cong C_m$. Thus $\mathbf{G}$ is cyclic. □

Problem 33.
Suppose that $\mathbf{D}$ is a commutative ring such that $\mathbf{D}[x]$ is a principal ideal domain. Prove that $\mathbf{D}$ is a field.

Proof. Let $d \in \mathbf{D}$, $d \neq 0$. We want to show that d has a multiplicative inverse. Let $I = (d, x)$, the ideal generated by d and x. Then $I = \{u(x) \cdot d + v(x) \cdot x \mid u(x), v(x) \in \mathbf{D}[x]\}$. Since $\mathbf{D}[x]$ is a principal ideal domain, we may write $I = (a(x))$ for some $a(x) \in \mathbf{D}[x]$. Notice that $d \in I$, so $a(x) \mid d$. This shows that $\deg a(x) = 0$. On the other hand, $x \in I$, so $a(x) \mid x$. Since x is irreducible in $\mathbf{D}[x]$, in other words, the only possible divisors of x are units and associates of x, we see that $a(x)$ is a unit. Therefore $1 \in I$. So, $I = \mathbf{D}[x]$. Also, notice that I is the set of polynomials whose constant term is a multiple of d. Since $1 \in I$, we conclude that 1 is a multiple of d. This means that d has a multiplicative inverse. So, $\mathbf{D}$ is a field. □

Problem 34.
Is the polynomial $y^3 - x^2y^2 + x^3y + x + x^4$ irreducible in $\mathbb{Z}[x, y]$?

Proof. Suppose that $P = y^3 - x^2y^2 + x^3y + x + x^4 = g(x, y)h(x, y)$ where $g, h \in \mathbb{Z}[x, y]$. Without loss of generality, assume that there exists a 1 term in g and an x term in h. Then there can not be an x, x^2, or x^3 term in g as multiplying any of these terms gives a term not in P. Similarly, there cannot be 1, y, y^2, or y^3 term in h. However, this contradicts y^3 being a term in p. Thus, P cannot not be factored. As the multiplicative inverse of P is $\frac{1}{P}$ and $\frac{1}{P}$ is not in $Z[x, y]$ we have P is not a unit. Thus, P is irreducible.

Alternatively, one can observe that $\mathbb{Z}[x, y] = (\mathbb{Z}[x])[y]$. Since $\mathbb{Z}$ is a unique factorization domain, $\mathbb{Z}[x]$ is a unique factorization domain. We can view the given polynomial as a polynomial in the indeterminate y having coefficients in the ring $\mathbb{Z}[x]$. Now, let $P = (x)$, the ideal of $\mathbb{Z}[x]$ generated by the element x. We see that P is a prime ideal and that x^2 and x^3 are elements of P, while 1 is not an element of P. Furthermore, observe that $P^2 = \{\sum_{i,j} x^{n_i} x^{n_j} \mid n_i \geq 1, n_j \geq 1\}$. Hence, $x + x^4$ is not an element of P^2. By Eisenstein's Criterion, we conclude that the specified polynomial is irreducible in $\mathbb{Z}[x, y]$. □

Problem 41.
Show that any integral domain satisfying the descending chain condition on ideals is a field.

Proof. Suppose R is an integral domain satisfying the descending chain condition on ideals. To show that R is a field, we must show the existence of multiplicative inverses for elements in R. To that end, let $a \in R$, $a \neq 0$, and consider the ideal (a). We then have

$$(a) \supseteq (a^2) \supseteq \cdots \supseteq (a^k) = (a^{k+1}) = \cdots$$

for some integer k. The ideal (a^{k+1}) is comprised of elements of the form $c \cdot a^{k+1}$ for some $c \in R$. Since $(a^k) = (a^{k+1})$, we have $a^k = d \cdot a^{k+1}$ for some $d \in R$. Then we have

$$\begin{aligned} d \cdot a^{k+1} - a^k = 0 &\Leftrightarrow (d \cdot a - 1) \cdot a^k = 0 \\ &\Leftrightarrow d \cdot a - 1 = 0 \\ &\Leftrightarrow d \cdot a = 1 \end{aligned}$$

So d is the multiplicative inverse of a, and thus R is a field. □

Problem 42.
Prove the following form of the Chinese Remainder Theorem: Let R be a commutative ring with unit 1 and suppose that I and J are ideals of R such that $I + J = R$. Then

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}.$$

Proof. Define $\phi : \frac{R}{I \cap J} \to \frac{R}{I} \times \frac{R}{J}$ by $\phi(\frac{r}{I \cap J}) = (\frac{r}{I}, \frac{r}{J})$.

Claim ϕ is well-defined.

Proof of Claim: Let $\frac{r}{I \cap J} = \frac{r'}{I \cap J}$. We see that

$$\begin{aligned} \frac{r - r'}{I \cap J} &= \frac{0}{I \cap J} \\ r - r' &\in I \cap J \end{aligned}$$

Now,

$$\begin{aligned} r - r' &\in I \\ \frac{r - r'}{I} &= \frac{0}{I} \\ \frac{r}{I} &= \frac{r'}{I} \end{aligned}$$

Similarly, $\frac{r}{J} = \frac{r'}{J}$. With these facts, we see

$$\begin{aligned}\phi(\frac{r}{I \cap J}) &= (\frac{r}{I}, \frac{r}{J}) \\ &= (\frac{r'}{I}, \frac{r'}{J}) \\ &= \phi(\frac{r'}{I \cap J})\end{aligned}$$

Claim ϕ is a homomorphism.

Proof of Claim: We see that ϕ respects addition

$$\begin{aligned}\phi(\frac{r}{I \cap J} + \frac{s}{I \cap J}) &= \phi(\frac{r+s}{I \cap J}) \\ &= (\frac{r+s}{I}, \frac{r+s}{J}) \\ &= (\frac{r}{I} + \frac{s}{I}, \frac{r}{J} + \frac{s}{J}) \\ &= (\frac{r}{I}, \frac{r}{J}) + (\frac{s}{I}, \frac{s}{J}) \\ &= \phi(\frac{r}{I \cap J}) + \phi(\frac{s}{I \cap J})\end{aligned}$$

and multiplication

$$\begin{aligned}\phi(\frac{r}{I \cap J} \cdot \frac{s}{I \cap J}) &= \phi(\frac{r \cdot s}{I \cap J}) \\ &= (\frac{r \cdot s}{I}, \frac{r \cdot s}{J}) \\ &= (\frac{r}{I} \cdot \frac{s}{I}, \frac{r}{J} \cdot \frac{s}{J}) \\ &= (\frac{r}{I}, \frac{r}{J}) \cdot (\frac{s}{I}, \frac{s}{J}) \\ &= \phi(\frac{r}{I \cap J}) \cdot \phi(\frac{s}{I \cap J})\end{aligned}$$

Claim $ker(\phi) = I \cap J$

Proof of Claim:

$$\begin{aligned}\frac{r}{I \cap J} \in ker(\phi) &\Leftrightarrow \phi(\frac{r}{I \cap J}) = (\frac{0}{I}, \frac{0}{J}) \\ &\Leftrightarrow r \in I \text{ and } r \in J \\ &\Leftrightarrow r \in I \cap J\end{aligned}$$

Claim $im(\phi) = \frac{R}{I} \times \frac{R}{J}$

Proof of Claim: Let $(\frac{r}{I}, \frac{r}{J}) \in \frac{R}{I} \times \frac{R}{J}$. We have $\phi(\frac{r}{I \cap J}) = (\frac{r}{I}, \frac{r}{J})$, so $(\frac{r}{I}, \frac{r}{J}) \in im(\phi)$.

Finally, invoking the Homomorphism Theorem, we have

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$$

□

Theorem 3 (**First Isomorphism Theorem**)**.**
Let $f : G \to H$ be a homomorphism with kernel K. Then K is a normal subgroup of G and $G/K \cong$ im f.

Theorem 4 (**Second Isomorphism Theorem**)**.**
If H and N are subgroups of G with N normal in G, then HN is a subgroup of G and

$$HN/N \cong H/(H \cap N).$$

Theorem 5 (**Third Isomorphism Theorem**)**.**
Let N and K be normal subgroups of G such that N is a subgroup of K. Then K/N is a normal subgroup of G/N and

$$(G/N)/(K/N) \cong G/K$$

Theorem 6 (**Lagrange's Theorem**)**.**
Let G be a group and let H be a subgroup of G. Then

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

In particular, if G is finite, then $|H|$ divides $|G|$.

Problem 1.
Let G be a finite group, let H be a subgroup of G, and let N be a normal subgroup of G. Suppose further that $|N|$ and $[G : N]$ are relatively prime and that $|H|$ divides $|N|$. Prove that $H \subseteq N$.

Proof. First, observe that $H \subseteq N \Leftrightarrow H = H \cap N \Leftrightarrow [H : H \cap N] = 1$. So we wish to show that $[H : H \cap N] = 1$. The Second Isomorphism Theorem tell us that

$$HN/N \cong H/(H \cap N)$$

So we have $[HN : N] = [H : H \cap N]$. Recall that $|N|$ and $[G : N]$ are relatively prime. So every factor of $|N|$ is relatively prime to every factor of $[G : N]$. In particular, since $|H|$ divides $|N|$, $|H|$ is relatively prime to every factor of $[G : N]$. But $[G : N] = [G : HN][HN : N]$. So $|H|$ is relatively prime to $[HN : N]$. Thus $|H|$ is relatively prime to $[H : H \cap N]$. However, Lagrange tells us that $[H : H \cap N]$ divides $|H|$. Therefore $[H : H \cap N] = 1$, and so $H \subseteq N$. □

Problem 2.
Let G be a finite group, let H be a subgroup of G, and let N be a normal subgroup of G. Suppose further that $|N|$ and $[G : N]$ are relatively prime and that $|H| = |N|$. Prove that $H = N$.

Proof. The Second Isomorphism Theorem tell us that

$$HN/N \cong H/(H \cap N)$$

so that $[HN : N] = [H : H \cap N]$. Now, $HN \leq G$, so Lagrange tells us that $[G : N] = [G : HN][HN : N]$. Since $[G : N]$ and $|N|$ are relatively prime, it follows that $[HN : N]$ and $|N|$ are relatively prime. Now, $[HN : N] = [H : H \cap N]$, so we see that $[H : H \cap N]$ and $|N|$ are relatively prime. Since $|N| = |H|$, it follows that $[H : H \cap N]$ and $|H|$ are relatively prime. However, Lagrange tells us that $[H : H \cap N]$ divides $|H|$. Thus $[H : H \cap N] = 1$. So $H = H \cap N$, and so $H \subseteq N$. Since $|H| = |N|$ and H, N are finite, we have $H = N$. □

Problem 3.
Let G be a finite group, let H be a subgroup of G, and let N be a normal subgroup of G. Suppose further that $|N|$ and $[G : H]$ are relatively prime. Prove that $N \subseteq H$.

Proof. By the Second Isomorphism Theorem, we have

$$HN/N \cong H/(H \cap N)$$

so that

$$\frac{|HN|}{|N|} = \frac{|H|}{|H \cap N|}.$$

Rearranging the terms, we have

$$\frac{|HN|}{|H|} = \frac{|N|}{|H \cap N|}.$$

Thus $[HN : H] = [N : H \cap N]$. By Lagrange, $[HN : H]$ divides $[G : H]$ since $HN \leq G$. Similarly, we have $[N : H \cap N]$ divides $|N|$. Since $|N|$ and $[G : H]$ are relatively prime, it follows that $[HN : H] = [N : H \cap N] = 1$, and thus $N = H \cap N$. Hence $N \subseteq H$. □

If $a \in G$, then we define the **centralizer** of a in G, denoted by $C_G(a)$, to be the set of all $g \in G$ that commute with a.

$$C_G(a) = \{g \mid g \in G \text{ and } gag^{-1} = a\}$$

It is immediate that $C_G(a)$ is a subgroup of G.

If $H \leq G$, then we define the **normalizer** of H in G, denoted by $N_G(H)$, to be

$$N_G(H) = \{a \mid a \in G \text{ and } aHa^{-1} = H\}$$

It is immediate that $N_G(H)$ is a subgroup of G. Also, notice that $H \lhd N_G(H)$. By definition, $N_G(H)$ is the largest subgroup of G in which H is normal.

Theorem 7 (**Sylow I**)**.**
Let G be a finite group, let p be a prime number, and let $k \in \mathbb{N}$. If $p^k \mid |G|$, then G has a subgroup of order p^k.

Theorem 8 (**Sylow II**)**.**
Let G be a finite group and let p be a prime.

a) All Sylow p-subgroups of G are conjugate. In particular, if P is a Sylow p-subgroup of G, then all Sylow p-subgroups of G are conjugate to P.

b) Let n_p denote the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$.

c) $n_p \mid [G : P]$ for any Sylow p-subgroup P of G.

d) If $H \leq G$ and $|H|$ is a power of p, then $H \leq P$ for some Sylow p-subgroup of G.

Problem 4. Let $p, q \in \mathbb{Z}$ be primes with $q \leq p$ and $p \not\equiv 1 \pmod{q}$. Prove that any group of order pq is abelian.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G. Since $|P| = p$ and $|Q| = q$, we have $P \cong \mathbb{Z}_p$ and $Q \cong \mathbb{Z}_q$. From the Sylow theorems, we have $n_p \equiv 1 \pmod{q}$ and $n_p \mid q$. Since $p \not\equiv 1 \pmod{q}$ and p, q are primes, we have $n_q = 1$ since $n_q \mid p$. (Otherwise $n_q = kq + 1 \equiv 1 \pmod{q}$).) So $n_q = 1$ gives us that Q is a unique, and hence normal Sylow q-subgroup of G. Similarly, we have $n_p = 1$ since $q \leq p$. Thus P is also a unique normal Sylow p-subgroup of G. Since $\gcd(p, q) = 1$, we have $P \cap Q = \{e\}$. From the isomorphism theorems, we get $PQ/Q \cong Q/(P \cap Q)$ and since $|P \cap Q| = 1$, $|PQ| = |P||Q|$. Thus $G = PG$, and so $G \cong P \times Q$ □

Problem 5.
Let G be a finite group and let $H \lhd G$ so that $|H| = p^k$ for some prime p and some positive integer k. Prove that H is contained in every Sylow p-subgroup of G.

Proof. Let G be a group with $p \mid |G|$. Since H is a p-subgroup of G, the Sylow theorems tell us that H is contained in some Sylow p-subgroup P of G. Now, for $g \in G$ we have $gHg^{-1} \subseteq gPg^{-1} = P'$, where P' is a Sylow p-subgroup of G. Thus every conjugate of H is contained in the corresponding conjugate of P. Now, H is a normal subgroup of G, so this means that H is contained in every conjugate of P. Thus H is contained in every Sylow p-subgroup of G. □

Problem 6.
Let G be a finite group and let P be a Sylow p-subgroup of G. Suppose that H is a p-subgroup of $N_G(P)$. Prove that $H \subseteq P$.

Proof. Recall

$$N_G(P) = \{g \in G \mid gPg^{-1} = P\}$$

We have $P \lhd N_G(P)$. Since H is a p-group, the Sylow theorems tell us that H is contained in some Sylow p-subgroup P'. Also by the Sylow theorems, we know that P and P' must be conjugates in $N_G(P)$. However, P is a normal subgroup of $N_G(P)$, so P is the unique Sylow p-subgroup of G. Thus $P = P'$, and hence $H \subseteq P$. □

Problem 7.
Let G be a finite group and let P be a Sylow p-subgroup of G, where p is a prime number. Prove that p and $[N_G(P) : P]$ are relatively prime.

Proof. We need to show that $p \nmid [N_G(P) : P]$. By the definition of Sylow p-subgroups, we know that $|P| = p^k$, where $p^k \mid |G|$ but $p^{k+1} \nmid |G|$. Now, by Lagrange, we have $|G| = [G : P]|P|$. Thus $p \nmid [G : P]$. Also by Lagrange, we have $[G : P] = [G : N_G(P)][N_G(P) : P]$, so we see that $p \nmid [N_G(P) : P]$. □

Problem 8. (Frattini Argument)
Let N be a normal subgroup of the finite group G, and let P be a Sylow p-subgroup of N. If $N_G(P)$ is the normalizer of P in G, show that $G = N_G(P)N$.

Proof. Let $g \in N_G(P)N$. As $N_G(P)$ and N are subgroups of G, we clearly have $g \in G$. Thus $N_G(P)N \subseteq G$. For the other direction, suppose $a \in G$. By normality of N, we have $a^{-1}Pa \subseteq a^{-1}Na = N$, so P and $a^{-1}Pa$ are conjugate Sylow p-subgroups of N. Thus there exists $n \in N$ so that

$$\begin{aligned} P &= n(a^{-1}Pa)n^{-1} \\ &= (an^{-1})^{-1}P(an^{-1}) \end{aligned}$$

From this, we conclude that $an^{-1} \in N_G(P)$, and so $a \in N_G(P)N$. Thus $G \subseteq N_G(P)N$. Hence $G = N_G(P)N$. □

Problem 9.
Let G be a nonabelian group. Prove that $G/Z(G)$ is not cyclic.

Proof. Recall that we define the **center** of G by

$$Z(G) = \{a \in G \mid ag = ga \quad \text{for every} g \in G]\}$$

We prove the contrapositive. Suppose that $G/Z(G)$ is cyclic. We need to show that G is abelian. Suppose $aZ(G)$ is a generator for $G/Z(G)$. Then if $g_1, g_2 \in G$, we have $g_1Z(G) = a^iZ(G)$ for some i. Thus we have $g_1(a^i)^{-1} = z_i \in Z(G)$. Similarly, we have $g_2Z(G) = a^jZ(G)$ for some j. So $g_2(a^j)^{-1} = z_2 \in Z(G)$. Since cyclic groups are abelian, we have

$$\begin{aligned} g_1g_2 &= a^iz_1a^jz_2 \\ &= z_1z_2a^{i+j} \\ &= z_2a_1a^{j+i} \\ &= z_2a^jz_1a^i \\ &= g_2g_1 \end{aligned}$$

We have shown that $g_1g_2 = g_2g_1$ for $g_1, g_2 \in G$. Thus G is an abelian group. □

Problem 10.
Prove that every finite nontrivial p-group has a nontrivial center.

Proof. Let P be a finite nontrivial p-group. Let P act on itself by conjugation. From the conjugacy class equation, we have

$$|P| = |Z(P)| + \sum_x [P : C(x)]$$

where the sum runs over conjugacy class representatives with $|orbit_x| > 1$. Now, $|P|$ is a prime power, and each $[P : C(x)]$ is divisible by p, so we must have $|Z(P)|$ divisible by p. Thus $|Z(P)| \neq 1$, and so $Z(P)$ is nontrivial. □

Problem 11.
Prove that the polynomial $y^3 - x^2y^2 + x^3y + x + x^4$ is irreducible in $\mathbb{Z}[x, y]$

Proof. Let

$$\begin{aligned} f &= y^3 - x^2y^2 + x^3y + x + x^4 \\ &= a_3y^3 + a_2y^2 + a_1y + a_0 \end{aligned}$$

Notice that x is an irreducible element of $\mathbb{Z}[x]$. So consider f as an element of $(\mathbb{Z}[x])[y]$. We have $x \mid a_2$, $x \mid a_1$, $x \mid a_0$, and $x \nmid a_3$. Also, we have $x^2 \nmid a_0$, so Eisenstein's criterion tells us that f is irreducible in $(\mathbb{Z}[x])[y] = \mathbb{Z}[x, y]$. □

Problem 12.
Prove that the polynomial $x^3y + x^2y - xy^2 + x^2 + y$ is irreducible in $\mathbb{Z}[x, y]$.

Proof. Let

$$\begin{aligned} f &= x^3y + x^2y - xy^2 + x^3 + y \\ &= (y + 1)x^3 + yx^2 + (-y^2)x + y \end{aligned}$$

Now, y is an irreducible element of $\mathbb{Z}[y]$, so consider f as an element of $(\mathbb{Z}[y])[z]$. Observe that $y \mid y$, $y \mid (-y^2)$, and $y \mid y$, but $y \nmid (y + 1)$. Also, $y^2 \nmid y$, so Eisenstein's criterion tells us that f is irreducible in $(\mathbb{Z}[y])[x] = \mathbb{Z}[x, y]$. □

Problem 13.
Let R be a commutative ring, and let

$$N = \{r \mid r \in R \text{ and } r^n = 0 \text{ for some positive integer n}\}.$$

a) Prove that N is an ideal of R.

b) Prove that $N \subseteq P$ for every prime ideal P of R.

Proof. **a)** Clearly $0 \in N$ since $0^1 = 0$ and we can take $n = 1$. Now, let $a \in N$ and $r \in R$. Pick n so that $a^n = 0$. Since we are in a commutative ring, we have $(ra)^n = r^n a^n = r^n 0 = 0$. Thus $ra \in N$. Now, suppose $a, b \in N$. We must show that $a + b \in N$. Pick positive integers m, n such that $a^m = b^n = 0$. We know that the Binomial Theorem holds in any commutative ring, so we have

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{n+m-k}$$

In each term in the sum above, either $a^k = 0$ or $b^{m+n-k} = 0$. This means $(a+b)^{m+n} = 0$, so $a + b \in N$ as desired.

b) Let P be a prime ideal and let $a \in N$. Then $a^n \in P$ for some n since $a^n = 0 \in P$. We argue by induction on n to show that $a \in P$. In the base step, we clearly have $a^1 = a \in P$. So suppose $a^k \in P$ for all $k \leq n$. Then we have $a^{k+1} = aa^k \in P$ since either $a \in P$ or $a^k \in P$ by the induction hypothesis. Thus $N \subseteq P$. □

Problem 14.
Let R be a commutative ring, let I be an ideal of R, and let

$$N = \{r \mid r \in R \text{ and } r^n \in I \text{ for some positive integer } n\}.$$

a) Prove that N is an ideal of R.

b) Prove that $N \subseteq P$ for every prime ideal P of R such that $I \subseteq P$.

Proof. **a)** First we check that N is an ideal. We see that $0 \in N$ since $0^1 = 0 \in I$ because I is an ideal. Next, if $r, s \in N$ we can pick positive integers m, n so that $r^n, s^m \in I$. Since the Binomial Theorem holds in commutative rings, we have

$$(r+s)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} r^k s^{m+n-k}$$

But observe that for all $k \leq m+n$ either $k \geq n$ or $m+n-k \geq m$. So in every case $r^k s^{m+n-k} \in I$. Consequently, $(r+s)^{m+n} \in I$. But this means that $r+s \in N$. Finally, let $r \in N$ with $r^n \in I$ and let $a \in R$. Then $(ar)^n = a^n r^n \in I$ since I is an ideal. This means $ar \in N$. Therefore N is an ideal.

b) Now, let P be a prime ideal such that $I \subseteq P$ and let $r \in N$. Pick a positive integer n so that $r^n \in I$. This implies that $r^n \in P$. We will induct on n to show that $r \in P$. The base step is clear. So suppose that $r^n \in P$ for all $n \leq k$. Then $r^{k+1} = rr^k \in P$ since either $a \in P$ or $a^k \in P$ by the induction hypothesis. Thus $N \subseteq P$. as desire. □

Zorn's Lemma

Zorn's Lemma is a transfinite existence principle which has found a number of useful and informative applications in algebra and analysis. While the the Lemma bears the name of Max Zorn, equal credit should be extended to Felix Hausdorff and Kazimierz Kuratowski who found closely related results decades before Zorn.

A **chain** or **linearly ordered set** is just a partially ordered set in which any two elements are comparable. We also refer to any subset of a partially ordered set as a **chain** when it is linearly ordered by the ordering inherited from the larger ordered set. This means that, where a and b are elements of the chain and $\leq$ denote the order relation, we have either $a \leq b$ or $b \leq a$. Let C be a subset of of a partially ordered set P and $b \in P$. We say that b is an **upper bound** of C provided $a \leq b$ for all $a \in C$. We say b is a **strict upper bound** provided $a < b$ for all a *in*C. An element d is **maximal** in C if $d \in C$ and whenever $d \leq a \in C$ it follows that $d = a$.

Zorn's Lemma *Let P be a partially ordered set and suppose that every chain in P has an upper bound in P. Then P has a maximal member.*

Problem 15.
Let R be a ring and let $a \in R$ so that $a^n \neq 0$ for every positive integer n. Prove that there is an ideal P with the following properties:

i) $a^n \notin P$ for all positive integers n

ii) If I is an ideal that properly includes P, then $a^m \in I$ for some positive integer m.

Proof. Let $\mathcal{F} = \{I \mid I \text{ is an ideal and } a^n \notin I \text{ for all positive integers } n\}$ We will invoke Zorn's Lemma to see that $\mathcal{F}$ has a maximal member P. This will finish the problem. All we need to do is establish that any chain in $\mathcal{F}$ (ordered by $\subseteq$) has an upper bound in $\mathcal{F}$.

Let $\mathcal{C}$ be a chain of ideals belonging to $\mathcal{F}$. We know that the union of any chain of ideals is again an ideal. So all we need to see is that $a^n \notin \bigcup \mathcal{C}$ for every positive integer n. If it were the case that $a^n \in \bigcup \mathcal{C}$, then we could pick $I \in \mathcal{C}$ so that $a^n \in I$. However, $I \in \mathcal{F}$ so we know that $a^n \notin I$. Thus $\bigcup \mathcal{C} \in \mathcal{F}$. So $\bigcup \mathcal{C}$ can serve as the desired upper bound in $\mathcal{F}$. Then Zorn tells us that $\mathcal{F}$ has a maximal member. □

Problem 16.
Let R be a ring, let I be an ideal of R, and let $a \in R$ so that $a^n \notin I$ for every positive integer n. Prove that there is an ideal P with the following properties:

i) $a^n \notin P$ for all positive integers n

ii) If J is an ideal that properly includes P, then $a^m \in J$ for some positive integer m.

Proof. Let $\mathcal{F} = \{K \mid K \text{ is an ideal with } I \subseteq K \text{ and } a^n \notin K \text{ for all positive integers } n\}$. Notice that $\mathcal{F}$ is not empty since $I \in \mathcal{F}$. Also notice that $\mathcal{F}$ is ordered by set inclusion. Let $\mathcal{C}$ be any chain in $\mathcal{F}$. We know that $\bigcup \mathcal{C}$ is an ideal, since the union of any chain of ideals is an ideal. Plainly, $\bigcup \mathcal{C}$ is an upper bound of $\mathcal{C}$ and also $\bigcup \mathcal{C}$ includes I. So to see that $\bigcup \mathcal{C} \in \mathcal{F}$, we only need that $a^n \notin \bigcup \mathcal{C}$ for each positive integer n. But since $a^n \notin K$ for all $K \in \mathcal{C}$, this follows immediately. So by Zorn's Lemma, there is P with is maximal in $\mathcal{F}$. Now, suppose J is an ideal that properly includes P. Then $J \notin \mathcal{F}$ by the maximality of P. This means that there must be a positive integer m so that $a^m \in J$. □

Problem 17.
Provide an example of a unique factorization domain that is not a principal ideal domain. Prove that your example has the desired properties.

Proof. Let F be any field. Then $F[x, y]$ is a UFD. Let I be ideal generated by $\{x, y\}$. So I consists of those polynomials with constant term 0. Suppose, for contradiction, that there exists a polynomial $p(x, y)$ that generates I. Then $p(x, y) \mid x$ and $p(x, y) \mid y$ and the constant term of $p(x, y)$ is 0. This means that there are polynomials $f(x, y)$ and $g(x, y)$ such that $x = f(x, y)p(x, y)$ and $y = g(x, y)p(x, y)$. Let the x-degree of a polynomial be the largest n such that x^n occurs in the polynomial. Similarly define the y-degree. Now, multiplying polynomials never decreases these degrees. So we find that $p(x, y)$ must have x-degree 0 since y has x-degree 0. Similarly, $p(x, y)$ must have y-degree 0 since x has y-degree 0. This means that neither x nor y occur in $p(x, y)$. Since the constant term of $p(x, y)$ is 0, we can only conclude that $p(x, y)$ is the zero polynomial. But the zero polynomial cannot generate I. So we have the desired contradiction.

Alternatively, one can show that $\mathbb{Z}[x]$ is a UFD but not a PID. Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[x]$ is also a UFD. Let I be the ideal generated by $\{2, x\}$. Suppose, for contradiction, that I is generated by a single element, say f. Then $f \mid 2$ and $f \mid x$, so there exist $g, h \in \mathbb{Z}[x]$ such that $fg = 2$ and $fh = x$. Now, $fg = 2$ shows that $f \in \mathbb{Z}$. Also $fh = x$ shows that $f = \pm 1$. Thus we must have $I = \mathbb{Z}[x]$. However, the constant term of every polynomial in $(x, 2)$ is a multiple of 2, so we see that $1 \notin (2, x) = I$. Thus I is a proper ideal of $\mathbb{Z}[x]$, and we have the desired contradiction. $\square$