Abstract

This document contains solutions to some of the problems appearing on comprehensive exams given by the Mathematics Department at the University of Hawaii over the past two decades. In solving many of these problems, I benefited greatly from the wisdom and guidance of Professor William Lampe. A number of other professors provided additional expert advice and assistance, for which I am very grateful. In particular, I thank Professor Ron Brown for leading an enlightening ring theory seminar in the fall of 2009, and Professor Tom Craven for taking over this job in the spring of 2010.

Some typographical and mathematical errors have surely found their way into the pages that follow. Nonetheless, I hope this document will be of some use to you as you explore two of the most beautiful areas of mathematics.

Finally, it's no secret that mathematics is best learned by solving problems. The purpose of this document, then, is to give you some problems to work on in order to locate any gaps in your understanding. The solutions are there to assist you in filling these gaps, and to provide cautionary notes about typical oversights and points of confusion.

Please send comments, suggestions, and corrections to: williandemeo@gmail.com.

Contents

1 Group Theory 3
   1.1 1993 November ................................................................. 3
   1.2 1999 March ................................................................. 6
   1.3 2002 November ............................................................... 8
   1.4 2003 November ............................................................... 11
   1.5 2004 November ............................................................... 12
   1.6 2006 April ................................................................. 14
   1.7 2006 November .......................................................... 17
   1.8 2007 April ................................................................. 18
   1.9 2008 January ............................................................... 19
   1.10 2008 April ................................................................. 20

2 Ring Theory 22
   2.1 1992 November ................................................................. 22
   2.2 1995 April ................................................................. 25
   2.3 1995 November .............................................................. 26
   2.4 1996 April ................................................................. 27
   2.5 1999 March ................................................................. 30
A Basic Definitions and Theorems

A.1 Algebras
A.2 Congruence Relations and Homomorphisms
A.3 Group Theory Basics
A.4 Direct Products
A.5 Ring Theory Basics
A.6 Factorization in Commutative Rings
A.7 Rings of Polynomials
A.8 Nakayama’s Lemma
A.9 Miscellaneous Results and Examples
1 Group Theory

1.1 1993 November

1. Prove that there is no non-abelian simple group of order 36.

Solution: Let $G$ be a group of order $|G| = 36 = 2^2 \cdot 3^2$. Then the Sylow theorem implies that $G$ has a subgroup $H$ of order $|H| = 9$. Define $G/H = \{gH : g \in G\}$, the set of left cosets of $H$ in $G$. This is a group if and only if $H \trianglelefteq G$, but let us assume that $H \ntrianglelefteq G$ (otherwise we’re done), in which case $G/H$ is merely a set of subsets of $G$. Note that the set $G/H$ contains exactly $|G : H| = |G|/|H| = 4$ elements. Denote by $\text{Sym}(G/H)$ the group of permutations of elements of $G/H$, and consider the map $\theta : G \to \text{Sym}(G/H)$, defined for each $g \in G$ by $\theta(g)(xH) = gxH$. The usual trivial calculation shows that this map is a homomorphism of $G$ into $\text{Sym}(G/H)$. In this case, it is obvious that $\theta$ cannot possibly be a monomorphism (embedding, or faithful representation) of $G$ in $\text{Sym}(G/H)$ since the order of $\text{Sym}(G/H) \cong S_4$ is 4! = 24, while $|G| = 36$. Therefore, $\theta$ must have a non-trivial kernel, $\ker \theta = \{g \in G | \theta(g) = \text{id}_{G/H}\} = \{g \in G | gxH = xH \text{ for all } x \in G\}$. Thus, $(e) \neq \ker \theta \trianglelefteq G$ (since the kernel of a homomorphism is a normal subgroup), so $G$ is not simple.

Remark: $A_5$ (which has order 60) is the smallest non-abelian simple group. \hfill \Box

2. Prove that for all $n \geq 3$, the commutator subgroup of $S_n$ is $A_n$.

3. a. State, without proof, the Sylow Theorems.

b. Prove that every group of order 255 is cyclic.

Solution:

Theorem. [L. Sylow (1872)] Let $G$ be a finite group with $|G| = p^m r$, where $m$ is a non-negative integer and $r$ is a positive integer such that $p$ does not divide $r$. Then

(i) $G$ has a subgroup of order $p^m$. Such a subgroup is called a Sylow $p$-subgroup of $G$.

(ii) If $H$ and $J$ are Sylow $p$-subgroups of $G$, then $J \leq gHg^{-1}$ for some $g \in G$. In particular, the Sylow $p$-subgroups of $G$ form a single conjugacy class.

(iii) Let $n_p$ denote the number of Sylow $p$-subgroups of $G$ and let $H$ be any Sylow $p$-subgroup of $G$. Then

$$n_p \equiv 1 \pmod{p}, \quad n_p \mid |G:H|, \text{ and } n_p = |G : N_G(H)|.$$  
(Note that $|G : H| = r$ so the second condition says that $n_p$ divides $r$.)

b. Let $G$ be a group of order $|G| = 255 = 3 \cdot 5 \cdot 17$. We will show that $G$ must be abelian. Then, the fundamental theorem of finitely generated abelian groups gives $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{17} \cong \mathbb{Z}_{255}$ (since 3, 5 and 17 are pairwise relatively prime), whence $G$ is cyclic.

For each $p \in \{3, 5, 17\}$, let $n_p$ denote the number of Sylow $p$-subgroups. By the Sylow theorems,

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 85 \quad \therefore \quad n_3 \in \{1, 85\},$$
$$n_5 \equiv 1 \pmod{5} \quad \text{and} \quad n_5 \mid 51 \quad \therefore \quad n_5 \in \{1, 51\},$$
$$n_{17} \equiv 1 \pmod{17} \quad \text{and} \quad n_{17} \mid 15 \quad \therefore \quad n_{17} = 1.$$  

In particular, the Sylow 17-subgroup is normal. \footnote{Recall, if $P$ is a Sylow $p$-subgroup, then so is $g^{-1}Pg$ ($\forall g \in G$). Thus, if $n_p = 1$, then $P = g^{-1}Pg$ ($\forall g \in G$), so $P$ is normal.}
1.1 1993 November

GROUP THEORY

Let $P_3$ denote an arbitrary Sylow $p$-subgroup. Note that $P_p \cap P_q = \{e\}$ for $p \neq q \in \{3, 5, 17\}$ since each non-identity element of $P_q$ generates $P_q$. Suppose both $n_3 = 85$ and $n_5 = 51$. Then, since $P_3 \cap P_5 = \{e\}$, a simple counting argument ($2 \cdot 85 + 4 \cdot 51 = 374 > 255$) shows that there are too many distinct group elements. Therefore, either $n_3 = 1$ or $n_5 = 1$ (or both).

Now note that $P_{17} \leq G$, so $G/P_{17}$ is a group of order $3 \cdot 5$, hence cyclic.\(^2\) Similarly, if $P_3 \leq G$, then $G/P_3$ is a group of order $5 \cdot 17$, hence cyclic, while if $P_5 \leq G$, then $G/P_5$ is a group of order $3 \cdot 17$, hence cyclic.

From here there are (at least) two ways to show that $G$ is abelian and complete the proof. One uses the commutator, and the other uses the following easily proved

**Lemma.** If $H \leq G$ and $K \leq G$, then $H \cap K \leq G$ and the natural map $\psi : G/(H \cap K) \rightarrow G/H \times G/K$ given by $\psi(g(H \cap K)) = (gh, gK)$ is a monomorphism.

(For the proof see Problem 3 of November 2004.)

By the lemma, we can embed $G/(H \cap K)$ (as a subgroup) in the group $G/H \times G/K$. Thus, take $H$ to be $P_{17}$, and $K$ to be either $P_3$ or $P_5$ (whichever is normal). Then $H \cap K = \{e\}$, so $G$ itself is (isomorphic to) a subgroup of the abelian group $G/H \times G/K$, and is therefore abelian.

Alternatively, recall that the commutator\(^3\) $G' \leq G$ is the unique minimal normal subgroup of $G$ such that $G/G'$ is abelian. (In particular, $G$ is abelian iff $G' = \{e\}$.) Therefore, since $G/P_{17}$ is abelian, $G' \leq P_{17}$. For the same reason, we have at least one of the following: $G' \leq P_3$ or $G' \leq P_5$. In any case, $G' \leq P_{17} \cap P_q = \{e\}$ for some $q \in \{3, 5\}$. Thus, $G$ is abelian.

\[\Box\]

4. Let $G$ be a group and let $X$ be a set. We say that $G$ acts on $X$ (on the left) if there is a multiplication $G \times X \rightarrow X$ such that $1x = x$ and $(gh)x = g(hx)$ for all $g, h \in G$ and $x \in X$.

a. Let $H$ be a subgroup of $G$. Prove that $G$ acts on the space of left cosets $G/H$.

b. Let $x \in X$ and let $H$ be the subgroup of $G$ fixing $x$. Define the orbit of $x$ under $G$ and prove that there is a one-to-one correspondence between this orbit and the space of left cosets $G/H$.

In what sense can this one-to-one correspondence be called an isomorphism?

c. Let $g \in G$ and let $x' = gx$. Let $H$ be the subgroup of $G$ fixing $x$ and let $H'$ be the subgroup fixing $x'$. Prove that $H$ and $H'$ are conjugate.

**Solution:**

a. Let $H$ be a subgroup of $G$, and let $X = G/H$ denote the set of left cosets of $H$ in $G$. Define $(g, xH) \mapsto gxH = (gx)H$ for each $g \in G$ and $xH \in X$. This is clearly well-defined. (Proof: If $(g_1, xH) = (g_2, yH)$, then $(g_1x)H = (g_2y)H$ because $(g_2y)^{-1}(g_1x) = y^{-1}x \in H$.) Also, this map takes $G \times X$ into $X$ and satisfies $1xH = xH$. Finally, by associativity of multiplication in $G$, we have $(gh)(xH) = ((gh)x)H = (g(hx))H = g(hxH)$.

b. Let $x \in X$ and let $H$ be the subgroup of $G$ fixing $x$. (This is called the stabilizer of $x$, and often denoted by $G_x$.) That is, $H := G_x := \{g \in G : gx = x\}$. The orbit of $x$ under $G$ is the set $Gx := \{gx : g \in G\}$. We prove that there is a one-to-one correspondence between this orbit and the set of left cosets $G/H$. Indeed, consider the map $G \ni g \mapsto gx \in Gx$, which is clearly surjective, and its kernel is given by the relation

\[\{(a, b) : a \in G \times G : ax = bx\} = \{(a, b) : b^{-1}ax = x\} = \{(a, b) : b^{-1}a \in H\} = \{(a, b) : aH = bH\}.

\(^2\)Recall, if $|G| = pq$ with $p < q$, both odd primes, and $p$ does not divide $q - 1$, then $G$ is cyclic.

\(^3\)The commutator, $G'$, is the subgroup generated by the set $\{aba^{-1}b^{-1} : a, b \in G\}$. 

4
In other words, $a$ and $b$ are in the same left $H$-coset iff they take $x$ to the same element of the orbit $\bar{G}x$. Equivalently, there is a one-to-one correspondence between the orbit of $x$ and the set of left cosets $G/H$.

The bijection is an isomorphism in the following sense: the algebra $\langle \bar{G}x; G \rangle$ is a transitive $G$-set, as is the algebra $\langle G/H; G \rangle$. The map $\varphi : (Gx; G) \to (G/H; G)$ given by $\varphi(ax) = aH$ is a well-defined bijection (by the argument above) and it respects the (unary) operations of the algebras; that is, for all operation symbols $a \in G$, and all $bx \in Gx$, we have $\varphi(a(bx)) = \varphi((ab)x) = (ab)H = a(bH) = a\varphi(bx)$. Thus, $\varphi$ is a $(G$-set) isomorphism.

(c) Let $g \in G$ and let $x' = gx$. Let $H$ be the subgroup of $G$ fixing $x$ and let $H'$ be the subgroup fixing $x'$. Then $H$ and $H'$ are conjugate, since

$$H' = \{a \in G : ax' = x'\} = \{a \in G : agx = gx\} = \{a \in G : g^{-1}agx = x\}$$
$$= \{gbg^{-1} \in G : bx = x\} = g\{b \in G : bx = x\}g^{-1} = gHg^{-1}.$$ 

5. Prove that a finite group is nilpotent if and only if it is a product of $p$-groups.

**Solution:** (See March 1999 Problem 4.)
1.2 1999 March

1. There is no simple group of order 328.

2. Every finite $p$-group has a nontrivial center.

3. Suppose $G$ is a group and $H$ is a subgroup of $G$ and $N$ is a normal subgroup of $G$.
   
   (a) If $G$ is solvable, then $H$ is solvable.
   (b) If $G$ is solvable, then $G/N$ is solvable.
   (c) If $N$ and $G/N$ are solvable, then $G$ is solvable.

4. Suppose $H$ and $K$ are subgroups of the group $G$. Then $[H,K]$ is the subgroup generated by $\{hkh^{-1}k^{-1} : h \in H \& k \in K\}$. We recursively define $G_n$ by $G_0 = G$ and $G_{n+1} = [G_n, G]$. A group is nilpotent iff for some $k$, $G_k = \{1\}$. Use this definition of nilpotent group in what follows. For the rest of the problem, $G$ is assumed to be a finite group.
   
   (a) If $P$ is a Sylow subgroup of $G$, then $N(N(P)) = N(P)$, where $N(P)$ denotes the normalizer of $P$.
   (b) If $G$ is a nilpotent group and $H$ is a subgroup of $G$ not equal to $G$, then $N(H) \neq H$.
   (c) If $G$ is nilpotent and $P$ is a Sylow subgroup of $G$, then $P$ is a normal subgroup of $G$.
   (d) If each of the Sylow subgroups of $G$ are normal in $G$, then $G$ is the direct product of its Sylow subgroups.
   (e) Every finite, nilpotent group is the direct product of its Sylow subgroups.

**Solution:** (a) Let $P$ be a Sylow $p$-subgroup of $G$. Of course, for any $H \leq G$, we have $H \leq N(H)$. In particular, $N(P) \leq N(N(P))$. To prove the reverse inclusion, fix $g \in N(N(P))$. That is, $g \in G$ and $gN(P)g^{-1} = N(P)$. Then, since $P \leq N(P)$, it follows that $gPg^{-1} \leq N(P)$. Also, $P$ and $gPg^{-1}$ are both Sylow $p$-subgroups of $G$, so they are both Sylow $p$-subgroups of $N(P)$. But $P \leq N(P)$, so $P$ is the unique Sylow $p$-subgroup of $N(P)$. Thus, $gPg^{-1} = P$. That is, $g \in N(P)$, which proves $N(N(P)) \leq N(P)$, as desired.

(b) $G$ is nilpotent iff there exists $n \in \mathbb{N}$ such that

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{e\}.$$ 

Now $G_n = \{e\} \leq H$ and, since $H$ is a proper subgroup, $G_0 = G \nless H$, so there is some $0 \leq k < n$ such that $G_{k+1} \leq H$ and $G_k \nless H$. Take any $x \in G_k \setminus H$. We complete the proof by showing that $x \in N(H)$. Indeed, $x \in G_k$ implies that, for any $h \in H$,

$$xhx^{-1}h^{-1} \in [G_k, G] = G_{k+1} \leq H.$$ 

so $xhx^{-1}h^{-1} \in H$. Therefore, $xhx^{-1} \in H$, for all $h \in H$. That is, $x \in N(H)$.

(c) Assume $G$ is nilpotent and $P$ is a Sylow subgroup of $G$. We show $P \leq G$. By (a), $N(N(P)) = N(P)$, and so (b) (with $H = N(P)$) implies that $N(P)$ cannot be a proper subgroup of $G$, so it must be all of $G$. That is, $N(P) = G$, which means $P \leq G$. 

(d) Let $P_1, \ldots, P_r$ be the Sylow subgroups of $G$ with orders $|P_i| = p_i^{e_i}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r$ are positive integers. Since $P_i \leq G$ for each $1 \leq i \leq r$, $P_1 \cdots P_r$ is a subgroup of $G$. If $a \in P_i$ has order $o(a)$, then $o(a) | p_i^{e_i}$, by Lagrange’s theorem. Since $p_1, \ldots, p_r$ are distinct primes, $o(a) \nmid p_j^{e_j}$, for $j \neq i$. Therefore, again by Lagrange’s theorem, $a \notin P_1 \cdots P_{i-1} P_{i+1} \cdots P_r$. This proves that, for each $1 \leq i \leq r$, $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_r) = (e)$. Finally, $P_1 \cdots P_r < G$ and $|P_1 \cdots P_r| = p_1^{e_1} \cdots p_r^{e_r} = |G|$ together imply that $G = P_1 \cdots P_r$. Therefore, by Corollary D.6. of the appendix, $G \cong P_1 \times \cdots \times P_r$. 
\qed
1.3 2002 November

1. Let $A$ be a finite abelian group. Let $n$ be the order of $A$ and let $m$ be the exponent of $A$ (i.e., $m$ is the least positive integer such that $ma = 0$ for all $a \in A$).
   a. Show that $m \mid n$ (i.e., $m$ is a factor of $n$).
   b. Show that $A$ is cyclic if and only if $m = n$.

2. Let $G$ be a finite group. Let $H \leq G$ be a subgroup.
   a. Show that the number of distinct conjugates of $H$ in $G$ is $|G|/|N(H)|$, where $N(H)$ is the normalizer of $H$ in $G$ and $|\cdot|$ indicates order.
   b. Show that $G = \bigcup_{g \in G} gHg^{-1}$ if and only if $H = G$.
   c. Deduce that $G$ is generated by a complete set of representatives of the conjugacy classes of elements of $G$.

Solution: a. Let $G$ act on $\text{Sub}[G]$, the set of subgroups of $G$, by conjugation. That is, for each $g \in G$ and $K \in \text{Sub}[G]$, let $K^g = gKg^{-1}$. The orbit and stabilizer of the subgroup $H$ under this action are, respectively,

\[ O_H = \{H^g : g \in G\} \quad \text{and} \quad \text{Stab}(H) = \{g \in G : H^g = H\} = N(H). \]

I claim that the index of $N(H)$ in $G$ is $[G : N(H)] = |O_H|$. Indeed, there is a one-to-one correspondence between the left cosets of $N(H)$ and the elements of $O_H$. This is verified as follows: for any $x, y \in G$,

\[ xN(H) = yN(H) \iff x^{-1}y \in N(H) \iff x^{-1}yH = Hx^{-1}y \iff yHy^{-1} = xHx^{-1}. \]

This proves that the map $xN(H) \mapsto xHx^{-1}$, from the cosets $G/N(H)$ to the orbit $O_H$, is well-defined and one-one. Therefore, $|O_H| = [G : N(H)] = |G|/|N(H)|$. \hfill \Box

b. We must show: $G = \bigcup_{g \in G} gHg^{-1}$ if and only if $H = G$.

For every $g \in G$, $|H| = |gHg^{-1}|$, so, for any $x, y \in G$, $|(xHx^{-1}) \cup (yHy^{-1})| \leq (|H| - 1) + (|H| - 1) + 1$ (at worst they intersect at the identity). More generally,

\[ \left| \bigcup_{g \in G} gHg^{-1} \right| \leq |G|(|H| - 1) + 1 \tag{1} \]

But, instead of using $|G|$ as a crude bound on the number of distinct conjugates of $H$, we can use the result from part a. That is,

\[ \left| \bigcup_{g \in G} gHg^{-1} \right| \leq \frac{|G|}{|N(H)|}(|H| - 1) + 1 \]

To finish the proof, we verify that

\[ \frac{|G|}{|N(H)|}(|H| - 1) + 1 \leq |G| \]

with equality if and only if $H = G$. 

8
Here’s a more concise proof which can be found, e.g., in Dixon [1] problem 1.9:

Let \( |G : H| = h \) and \( |G| = n \). Since \( H \leq N(H) \), therefore, by 1.1.3, \( H \) has at most \( h \) conjugates in \( G \). Since all subgroups have the identity element in common, the number of distinct elements in these conjugates of \( H \) is at most \( 1 + (|H| - 1)h = n - h + 1 < n \).

c. Deduce that \( G \) is generated by a complete set of representatives of the conjugacy classes of elements of \( G \).

3. Let \( p, q \) and \( r \) be distinct prime numbers.
   a. List, up to isomorphism, all abelian groups of order \( p^4 \).
   b. Up to isomorphism, how many abelian groups of order \( p^4q^4r^3 \) are there?

4. Let \( G \) be a nonsolvable group of least order among nonsolvable groups. Show that \( G \) is simple.

Solution: Let \( G \) be a group satisfying the hypothesis and suppose \( G \) is not simple. Then there is a proper nontrivial normal subgroup \( N \trianglelefteq G \). Now \( |N| < |G| \) and \( |G/N| < |G| \), so \( N \) and \( G/N \) are both solvable (by the minimality hypothesis). But this implies that \( G \) is solvable. (By Problem 3 of March 1999, \( G \) is solvable iff \( N \) and \( G/N \) are solvable). This contradiction completes the proof. \( \square \)

5. Let \( G \) be a group of order \( p^nm \), where \( p \) is a prime number, \( n \geq 1 \) and \( p \) is not a factor of \( m \). Let \( r \) be the number of Sylow \( p \)-subgroups of \( G \) and let \( E = \{K_1, \ldots, K_r\} \) be the set of Sylow \( p \)-subgroups of \( G \). Let \( N(K_i) \) be the normalizer of \( K_i \) in \( G \), and let \( G \) act on \( E \) by conjugation.
   a. Show that \( \bigcap_{i=1}^r N(K_i) \) is a normal subgroup of \( G \).
   b. Show that \( |\bigcap_{i=1}^r N(K_i)| \geq p^n/(r-1)! \)
   c. Deduce that a group of order 48 is not simple.

Solution: a. By definition, 
   \[ N(K_i) = \{g \in G : K_i^g = K_i\} \]
   where \( K_i^g = gK_ig^{-1} = \tau_g(K_i) \) are various common notations for the action (on \( E \)) of conjugation by \( G \). (The subgroup \( N(K_i) \) is sometimes called the stabilizer of \( K_i \) under this action.) Let \( \tau : G \to \text{Sym}(E) \) be the map which sends each \( g \in G \) to the action \( \tau_g \in \text{Sym}(E) \), the group of permutations on the set \( E \). It is trivial to check that \( \tau \in \text{Hom}(G, \text{Sym}(E)) \), with kernel
   \[ \ker \tau = \{g \in G : K_i^g = K_i \text{ for all } K_i \in E\} = \bigcap_{i=1}^r N(K_i). \]
   As kernels of homomorphisms are normal subgroups, \( 4 \bigcap_{i=1}^r N(K_i) \trianglelefteq G \).

b. By part a. and the first isomorphism theorem,
   \[ G/\bigcap_{i=1}^r N(K_i) \cong \text{im}\tau \leq \text{Sym}(E) \]

---

\(^4\)In fact, the set of all kernels of homomorphisms of a group is precisely the set of all normal subgroups of the group.
Therefore, $|G|/|\bigcap N(K_i)| \leq |\text{Sym}(E)| = r!$. That is,

$$\frac{p^nm}{r!} \leq |\bigcap N(K_i)|.$$

To finish the proof of part b., then, we need only show $p^n/(r - 1)! \leq p^nm/r!$; equivalently, $r \leq m$. In other words, we must show that the number $r$ of Sylow $p$-subgroups is at most $m$. The Sylow theorem implies that $r$ divides $[G : K]$, for any Sylow $p$-subgroup $K$. In the present case $|K| = p^n$, so $[G : K] = m$. Thus $r$ divides $m$, so $r \leq m$, as desired.

c. To deduce that a group of order 48 is not simple, suppose $|G| = 48 = 2^4 \cdot 3$, and, as above, let $r$ denote the number of Sylow 2-subgroups of $G$, and denote these subgroups by $\{K_1, \ldots, K_r\}$. Then the subgroup $\bigcap_{i=1}^{r} N(K_i)$ is normal in $G$ (by a.) and has order at least $2^4/(r - 1)!$ (by b.). The Sylow theorem implies that $r$ divides $[G : K] = |G|/|K_i| = 48/2^4 = 3$, so $r \in \{1, 3\}$. In either case, $|\bigcap N(K_i)| \geq 2^4/(r - 1)! > 1$, which proves that $\bigcap N(K_i)$ is a nontrivial normal subgroup of $G$, so $G$ is not simple.

6. Show that a finite group $G$ is nilpotent if and only if $G$ is isomorphic to the product of its Sylow $p$-subgroups.
1. Let $H$ be a finite index subgroup of $G$. Show that there exists a finite index subgroup $K$ of $G$ such that $K \subseteq H$ and $K$ is normal in $G$.

2. Let $G$ be a group of order 84. Show that $G$ is not simple.

3. Let $G$ be a group and let $A$ be an abelian normal subgroup of $G$. Show that there is a nontrivial homomorphism from $G/A$ to the automorphism group of $A$.

4. State what it means for a group to be solvable, and show that any group of order 280 is solvable.

5. Prove that a group of order 343 has a nontrivial center.
1.5 2004 November

1. a. Carefully state (without proof) the three Sylow theorems.

b. Prove that every group of order \( p^2q \), where \( p \) and \( q \) are primes with \( p < q \) and \( p \) does not divide \( q - 1 \), is abelian.

c. Prove that every group of order 12 has a normal Sylow subgroup.

2. a. Among finite groups, define nilpotent group, in terms of a particular kind of normal series. State two conditions on \( G \) which are equivalent to the condition that \( G \) is nilpotent.

b. Prove that the center \( Z(G) \) of a nilpotent group is non-trivial.

c. Give an example which shows that \( N \trianglelefteq G \) with both \( N \) and \( G/N \) nilpotent is not sufficient for \( G \) to be nilpotent.

3. a. If \( K, L \) are normal subgroups of \( G \) prove that \( G/K \cap L \) is isomorphic to a subgroup of \( G/K \times G/L \) (the external direct product). What is the index of this subgroup in \( G/K \times G/L \), in terms of \( [G : K] \), \( [G : L] \) and \( [G : KL] \)?

b. Prove either direction of: If \( N \trianglelefteq G \), then \( G \) is solvable if and only if both \( N \) and \( G/N \) are solvable.

Solution: a. Define the natural mapping

\[
G/K \cap L \ni g(K \cap L) \mapsto (gK, gL) \in G/K \times G/L.
\]

We must check that this mapping is well-defined and one-to-one, as follows:

\[
x(K \cap L) = y(K \cap L) \iff x^{-1}y \in K \cap L \\
\implies x^{-1}y \in K \quad \text{and} \quad x^{-1}y \in L \\
\implies xK = yK \quad \text{and} \quad xL = yL \\
\implies (xK, xL) = (yK, yL).
\]

To be clear, the forward implications \((\Rightarrow)\) prove well-definedness, the reverse implications \((\Leftarrow)\) one-to-one-ness.

Also, it is important to note that these calculations take \( G/K, G/L, \) and \( G/K \cap L \) to be groups, with multiplications given by \( xK yK = xyK \), etc. This requires that the subgroups \( K \) and \( L \), and hence \( K \cap L \), be normal.

If, for example, \( K \) were not normal, then \( G/K \) would not be a group.

It remains to check that the mapping is a homomorphism. Let \( \varphi \) denote the mapping, and fix two cosets \( x(K \cap L) \) and \( y(K \cap L) \) in \( G/(K \cap L) \). Then

\[
\varphi(x(K \cap L)y(K \cap L)) = \varphi(xy(K \cap L)) = (xyK, xyL) = (xK, xL)(yK, yL) = \varphi(x(K \cap L)) \varphi(y(K \cap L)).
\]

By exhibiting a monomorphism \( \varphi : G/K \cap L \hookrightarrow G/K \times G/L \), we have proved that \( G/K \cap L \) can be embedded as a subgroup in \( G/K \times G/L \).

The index of \( G/K \cap L \) in \( G/K \times G/L \), in terms of \( [G : K], [G : L] \) and \( [G : K \cap L] \), is

\[
\frac{[G/K \times G/L]/[G/K \cap L]}{[G/K]/[K \cap L]} = \frac{[G/K][G/L]}{[G/K \cap L]}.
\]

\( \square \)

\(^5\text{cf. problem 3, November 2006, and others.}\)
b. (See Problem 3 of March 1999 exam.)

4. a. If $H$ is a subgroup of $G$ and $[G : H] = n > 2$, prove that there exists a homomorphism $\rho$ from $G$ into $S_n$, the group of all permutations of an $n$-element set. Show that the kernel of $\rho$ is contained in $H$, and the image of $\rho$ is a transitive subgroup of $S_n$.

b. If $[G : H] = n$ and $G$ is simple, then $G$ is isomorphic to a subgroup of $A_n$, the subgroup of all even permutations.

c. Every group of order $2^3 \cdot 3^2 \cdot 11^2$ is solvable.

5. Let $G$ be a finite group, and suppose the automorphism group of $G$, $\text{Aut}(G)$, acts transitively on $G \setminus \{1\}$. That is, whenever $x, y \in G \setminus \{1\}$ there exists an automorphism $\alpha \in \text{Aut}(G)$ such that $\alpha(x) = y$. Prove that $G$ is an elementary abelian $p$-group for some prime $p$, by proving that:

a. All non-identity elements of $G$ have order $p$, for some prime $p$.

b. Here $Z(G) \neq 1$, and the center of every group is a characteristic subgroup.

c. Thus $G \neq Z(G)$, i.e., $G$ is abelian.

6. Suppose $N$ is a normal subgroup of $G$. $C_G(N)$ denotes $\{g \in G \mid g^{-1}ng = n \text{ for each } n \in N \}$.

a. Prove that $C_G(N) \subseteq G$, and if $C_G(N) = \{1\}$ then $|G|$ divides $|N|!$.

b. If $N$ is also cyclic, prove that $G/C_G(N)$ is abelian, and hence that $G' \leq C_G(N)$, where $G'$ is the commutator subgroup of $G$. 
1.6 2006 April

Instructions: Do as many problems as you can. You are not expected to do all of the problems. You may use earlier parts of a problem to solve later parts, even if you cannot solve the earlier part; however, complete solutions are preferred. Most importantly, give careful solutions.

1. Show that there is no simple group of order 992.

Solution: Suppose $G$ is a group of order $|G| = 992 = 2^5 \cdot 31$. Our goal is to show that $G$ contains a normal subgroup. By the Sylow theorems, the number $n_p$ of Sylow $p$-subgroups satisfies

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid [G : H]$$

where $H$ is any Sylow $p$-subgroup. Therefore, $n_{31} \equiv 1 \pmod{31}$ and $n_{31} \mid 32$, so $n_{31} \in \{1, 32\}$. If $n_{31} = 1$, this means there is a unique Sylow 31-subgroup, which must be normal in $G$ (since conjugates of Sylow $p$-subgroups are also Sylow $p$-subgroups).

Suppose $n_{31} = 32$. Now, any element of a group of prime order generates the whole group. Therefore, the Sylow 31-subgroups must intersect at the identity. Thus, there are $30 \cdot 32 = 960$ elements of order 31 in $G$. This leaves only 32 elements in $G$ that are not of order 31. Also, $G$ must contain a Sylow 2-subgroup of order $2^5 = 32$. Apparently, only one of these can fit inside $G$, so $n_2 = 1$ (since this results in exactly $992 = 960 + 32$ elements). In this case, it is the Sylow 2-subgroup that is unique, hence normal in $G$. \hfill \Box

2. Let $G$ be a nonabelian simple group. Let $S_n$ be the symmetric group of all permutations on an $n$-element set, and let $A_n$ be the alternating group.

a. Show that if $G$ is a subgroup of $S_n$, $n$ finite, then $G$ is a subgroup of $A_n$.

b. Let $H$ be a proper subgroup of $G$, and, for $g \in G$, let $\lambda_g$ be the map of the set of left cosets of $H$ onto themselves defined by $\lambda_g(xH) = gxH$. Show that the map $g \mapsto \lambda_g$ is a monomorphism (injective homomorphism) of $G$ into the group of permutations of the set of left cosets of $H$.

c. Let $H$ be a subgroup of $G$ of finite index $n$ and assume $n > 1$ (so $H \neq G$). Show that $G$ can be embedded in $A_n$.

d. If $G$ is infinite, it has no proper subgroup of finite index.

e. There is no simple group of order 112.

Solution: a. Suppose $G$ is a subgroup of $S_n$, $n$ finite, and assume $G$ is nonabelian and simple. Clearly $G \neq S_n$, since $S_n$ is not simple (for example, $A_n \triangleleft S_n$). Consider $G \cap A_n$. This is easily seen to be a normal subgroup of $G$. (Normality: if $\sigma \in G \cap A_n$ and $g \in G$, then $g\sigma g^{-1} \in G$ and $g\sigma g^{-1} \in A_n$, since $A_n \triangleleft S_n$, so $g\sigma g^{-1} \in G \cap A_n$.) Therefore, as $G$ is simple, either $G \cap A_n = (e)$ or $G \cap A_n = G$. In fact, $G \cap A_n = (e)$ never occurs under the given hypotheses, and two proofs of this fact are given below. In case $G \cap A_n = G$, of course, $G \leq A_n$ and we are done.

Proof 1: Suppose $G \cap A_n = (e)$. Then $G$ contains only $e$ and odd permutations. Let $\zeta \in G$ be an odd permutation. Then $\zeta^2$ is an even permutation in $G$, so it must be $e$. Thus, every nonidentity element of $G$ has order 2. Suppose $\eta$ is another odd permutation in $G$. Then $\zeta \eta$ is an even permutation in $G$, so $\zeta \eta = e$. Therefore, $\zeta \zeta = e = \zeta \eta$, so $\eta = \zeta$. This shows $G$ has only two elements $e$ and $\zeta$. But then $G \cong \mathbb{Z}_2$ is abelian, contradicting our hypothesis.

\footnote{The notation $a \mid b$ means $a$ evenly divides $b$, i.e. $ac = b$ for some $c$.}
Proof 2: If $G$ were not a subgroup of $A_n$, then the group $GA_n \leq S_n$ would have order larger than $|A_n| = |S_n|/2$. By Lagrange’s theorem, then, it would have order $|S_n|$. Therefore, $GA_n = S_n$, and, by the second isomorphism theorem,

$$G/(G \cap A_n) \cong GA_n/A_n = S_n/A_n.$$ 

This rules out $G \cap A_n = (e)$, since that would give $G \cong S_n/A_n \cong \mathbb{Z}_2$ (abelian), contradicting the hypothesis. □

Remark: Although the first proof above is completely elementary, the second is worth noting since it reveals useful information even when we don’t assume $G$ is simple and nonabelian. For example (Rose [6], page 77), if $G$ is a subgroup of $S_n$ containing an odd permutation, then we can show that exactly half of the elements of $G$ are even and half are odd. Indeed, under these conditions we easily get that a group of order 112 cannot be simple.

b. Let $H \leq G$, and let $S$ denote the set of left cosets of $G$. Let $\text{Sym}(S)$ denote the group of permutations of $S$. Then the map $\lambda : G \to \text{Sym}(S)$ – defined by $\lambda(g) = \lambda_g$, where $\lambda_g(xH) = gxH$ – is a monomorphism of $G$ into $\text{Sym}(S)$. To prove this, we first show that $\lambda(g) = \lambda_g$ is indeed a bijection of $S$, then we show that $\lambda$ is a homomorphism of $G$, and finally we show that $\ker \lambda = (e)$.

To see that $\lambda_g$ is injective, observe

$$\lambda_g(xH) = \lambda_g(yH) \iff gxH = gyH \iff (gy)^{-1}gx \in H \iff y^{-1}x \in H \iff xH = yH.$$ 

To see that $\lambda_g$ is surjective, fix $xH \in S$, and notice that $\lambda_g(g^{-1}xH) = gg^{-1}xH = xH$.

To see that $\lambda$ is a homomorphism, note that, for any $xH \in S$,

$$\lambda_{g_1 g_2}(xH) = g_1 g_2 xH = \lambda_{g_1}(g_2 xH) = \lambda_{g_1} \circ \lambda_{g_2}(xH).$$ 

That is, $\lambda(g_1 g_2) = \lambda(g_1) \lambda(g_2)$, which proves that $\lambda$ is a homomorphism.

Finally, note that $\ker \lambda$ is a normal subgroup of $G$. Therefore, as $G$ is simple, either $\ker \lambda = (e)$, or $\ker \lambda = G$. But

$$\ker \lambda = \{g \in G : \forall x \in G, \lambda_g(xH) = xH\} = \{g \in G : \forall x \in G, x^{-1}gx \in H\} \leq H$$ 

(since $e \in G$). Therefore, $H \neq G$, so $\ker \lambda \neq G$, so $\ker \lambda = (e)$. This proves that $\lambda$ is a monomorphism. □

c. Let $H$ be a subgroup of $G$ of finite index $n$ and assume $n > 1$ (so $H \neq G$). We must show that $G$ can be embedded into $A_n$.

Part b. showed that $\lambda$ embeds $G$ into $\text{Sym}(S)$, where $S$ is the set of left cosets of $H$ in $G$. Now $[G : H] = |S| = n$, which implies that $\text{Sym}(S) \cong S_n$, the group of permutations of $n$ elements. Therefore, $G$ is isomorphic to a subgroup of $S_n$. By part a., then, $G$ is isomorphic to a subgroup of $A_n$. □

d. Suppose $G$ is infinite. We must show it has no proper subgroup of finite index. If, on the contrary, $H \leq G$ with $[G : H] = n$, then $G$ would be isomorphic to a subgroup of the finite group $A_n$. Impossible. □

e. Suppose, by way of contradiction, that $G$ is a simple subgroup with $|G| = 112 = 2^4 \cdot 7$. Clearly, $G$ is nonabelian. (Proof: $|G|$ is not prime, so $G$ has nontrivial proper subgroups. Also, $G$ is simple, while if $G$ were abelian, all subgroups would be normal.) Now, the Sylow theorems imply that $G$ has a Sylow 2-subgroup of order 2$^4$, call it $H$. Then $[G : H] = 7$, so, by part c., $\lambda : G \to A_7$. Thus $G$ is (isomorphic to) a subgroup of $A_7$ and $|A_7| = 7! = 7 \cdot 5 \cdot 3^2 \cdot 2^3$. By Lagrange’s theorem, $|G|$ divides $|A_n|$. But, 2$^4 \cdot 7$ does not divide 2$^4 \cdot 3^2 \cdot 5 \cdot 7$. This contradiction proves that a group of order 112 cannot be simple. □
3. a. Let \( \alpha \) be an element of the symmetric group \( S_n \) and let \((i_1 i_2 \ldots i_k)\) be a cycle in \( S_n \). Prove that \( \alpha^{-1}(i_1 i_2 \ldots i_k)\alpha = (i_1 \alpha i_2 \alpha \ldots i_k \alpha) \). [Note that it is assumed that permutations act on the right, so \( \alpha \) maps \( i \) to \( i\alpha \).]

b. Show that \( A_4 \) is not simple.

c. Show that any five-cycle \( \sigma \in S_5 \) and any two-cycle \( \tau \in S_5 \) together generate \( S_5 \).

4. If \( A \) and \( B \) are subgroups of a group \( G \), let \( A \lor B \) be the smallest subgroup containing both, and let \( AB = \{ab : a \in A, b \in B\} \).

a. Show that if \( A \) is a normal subgroup then \( AB = A \lor B \) and that, if both \( A \) and \( B \) are normal, then \( A \lor B \) is normal.

b. If \( A, B \) and \( C \) are normal subgroups of \( G \) and \( C \subseteq A \), prove Dedekind’s modular law:
\[
A \cap (B \lor C) = (A \cap B) \lor C
\]

5. Let \( G \) be a group and let \( Z \) be its center.

a. Show that if \( G/Z \) is cyclic then \( G \) is abelian.

b. Show that any group of order \( p^2 \), where \( p \) is a prime, is abelian.

c. Give an example of a non-abelian group \( G \) where \( G/Z \) is abelian.

d. Let \( \varphi \) be a homomorphism from \( G \) onto \( K \), where \( K \) is an abelian group. Let \( N \) be the kernel of \( \varphi \) and suppose \( N \) is contained in \( Z \). Suppose that there is an abelian subgroup \( H \) of \( G \) such that \( \varphi(H) = K \). Show \( G \) is abelian.

6. Let \( G \) be a finite group and let \( H \trianglelefteq G \) be a normal subgroup. Show that \( G \) is solvable if and only if \( H \) and \( G/H \) are solvable.
1.7 2006 November
1. Find (up to isomorphism) all groups with at most fifteen elements.

2. Let $G$ be a finitely generate group.
   a. Prove that every proper subgroup $H < G$ is contained in a maximal proper subgroup.
   b. Show that the intersection of the maximal proper subgroups of $G$ is a normal subgroup.

3. a. Carefully state (without proof) the three Sylow theorems.
   b. Prove that every group of order $p^2q$, where $p$ and $q$ are primes with $p < q$ and $p$ does not divide $q - 1$, is abelian.

4. Prove that the center of a finite abelian $p$-group is nontrivial.

5. Let $G$ be a group and $H$ a subgroup of $G$, $N$ a normal subgroup of $G$. Show that $HN$ is a subgroup of $G$, that $H \cap N$ is a normal subgroup of $H$, and that $HN/N \cong H/H \cap N$.

7cf. problem 1, November 2004, and others.
1. Let $H$ and $K$ be (not necessarily normal) subgroups of a group $G$. For $g$ an element of $G$ the set $HgK$ is called a double coset. Show that any two double cosets are either identical or do not intersect.

2. State (without proof) the three Sylow theorems. Show that every group of order 56 contains a proper normal subgroup.

3. Define $G'$, the commutator subgroup of $G$. Show that $G'$ is a normal subgroup of $G$. Show that every homomorphism from $G$ to an abelian group $A$ factors through $G/G'$ (i.e., given $\varphi : G \rightarrow A$ there exists $\bar{\varphi} : G/G' \rightarrow A$ such that $\varphi = \bar{\varphi} \circ \pi$ where $\pi : G \rightarrow G/G'$ is natural).

4. Short answers.
   a. Give examples of groups $K$, $N$, and $G$ with $K$ a normal subgroup of $N$, $N$ a normal subgroup of $G$, but $K$ not a normal subgroup of $G$.
   b. Give an example of a simple group that is not cyclic.
   c. Give an example of a solvable group that is not nilpotent.
   d. Give an example of a group $G$ that is not abelian but $G/C(G)$ is abelian where $C(G)$ denotes the center of $G$.
   e. Make a list of abelian groups of order 72 such that every abelian group of order 72 is isomorphic to exactly one group on your list.
   f. Give a solvable series for $S_4$, the symmetric group on four elements.

5. Let $H$ be a finite index subgroup of $G$. Show there is a normal subgroup of $G$ that is contained in $H$ and has finite index in $G$. 
1.9 2008 January

Instructions: Do as many problems as you can. You may use earlier parts of a problem to solve later parts, even if you cannot solve the earlier part; however, complete solutions are preferred. Most importantly, give careful solutions.

1. Prove that if $H$ is a subgroup of a finite group $G$, then $|H|$ divides $|G|$ and use this to show that the order of each element of a finite group divides the order of the group.

2. a. State Sylow’s theorems.
   b. Show that there is no simple group of order 56.
   c. Show that every group of order 35 has a normal subgroup of order 5 and one of order 7.
   d. Is every group of order 35 abelian?

3. How many nilpotent groups of order 360 are there? Justify your answer. Your justification should indicate clearly which theorems you are applying. If you are not able to find the number of nilpotent groups, at least find the number of Abelian groups of order 360.

4. Show that every group of order 1000 is solvable. You can use the fact that if $G$ has a normal subgroup $N$ such that both $N$ and $G/N$ are solvable, then $G$ is solvable.
1.10 2008 April

1. Prove that $S_4$ is solvable but not nilpotent.

Preliminaries: The symmetric group on four letters, $S_4$, contains the following permutations (here we use $\{0, 1, 2, 3\}$ to denote the four letters that the elements of $S_4$ permute):

<table>
<thead>
<tr>
<th>permutations</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>(01), (02), (03), (12), (13), (23)</td>
<td>2-cycles</td>
</tr>
<tr>
<td>(01)(23), (02)(13), (03)(12)</td>
<td>product of 2-cycles</td>
</tr>
<tr>
<td>(012), (013), (021), (023), (031), (032), (123), (132)</td>
<td>3-cycles</td>
</tr>
<tr>
<td>(0123), (0132), (0213), (0231), (0312), (0321)</td>
<td>4-cycles</td>
</tr>
</tbody>
</table>

The set of subgroups of $S_4$, denoted by $\text{Sub}[S_4]$, contains 30 elements. In particular, there is the alternating group, $A_4$, which has 12 elements and is generated by the 3-cycles in the table above. The alternating group consists of the “even” permutations, which are the permutations that can be written as a product of an even number of 2-cycles or “transpositions.” For example, $(012) = (02)(01)$, $e = (01)(01)$, are even, while $(01)$ and $(0123) = (03)(02)(01)$ are odd. Thus, the 12 elements of $A_4$ are (from the table above): the eight 3-cycles, the three products of disjoint 2-cycles, and the identity.

Another important subgroup is the Klein four group $V_4$. This is the subgroup of $A_4$ generated by the three products of disjoint 2-cycles; that is, $V_4 = \{e, (01)(23), (02)(13), (03)(12)\}$. It is useful to note that $V_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, and the subgroup lattice $\text{Sub}[V_4]$ is the five element modular lattice $M_3$. That is, $V_4$ has three subgroups $\{e, (01)(23)\}$, $\{e, (02)(13)\}$, and $\{e, (03)(12)\}$, and each pair meets at the identity and joins to $V_4$.

Solution: We know that $S_4$ is solvable simply because we can write down a normal series, $(e) \trianglelefteq \{e, (12)\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$, with abelian factors:

$\{e, (12)\}/(e) \cong \mathbb{Z}_2, \quad V_4/\{e, (12)\} \cong \mathbb{Z}_2, \quad A_4/V_4 \cong \mathbb{Z}_3, \quad S_4/A_4 \cong \mathbb{Z}_2.

In fact, the factors of the subnormal series are cyclic, which is more than we need.

We now prove that $S_4$ is not nilpotent. Let $C_0 = (e), C_1 = Z(G)$ (the center of $G$), and let $C_2 = \pi_1^{-1}(Z(G/C_1))$ where $\pi_1: G \twoheadrightarrow G/C_1$ is the canonical projection epimorphism. That is, $C_2$ is defined to be the (unique) normal subgroup of $G$ such that $C_2/C_1 = Z(G/C_1)$. Given $n$, define $C_{n+1} = \pi_n^{-1}(Z(G/C_n))$. Then, by definition, $G$ is nilpotent if and only if there is an $n \in \mathbb{N}$ such that $C_n = G$. The series $(e) < C_1 < C_2 < \cdots < C_n = G$ is called the ascending central series.

We claim that the center of $S_4$ is trivial. That is, $Z(S_4) = (e)$. Once we prove this, then it is clear that $S_4$ is not nilpotent. For the ascending central series never gets off the ground in this case, so it has no chance of ever reaching $S_4$.

Recall, if $N \trianglelefteq G$ and $G/N$ is cyclic and $N \subseteq Z(G)$, then $G$ is abelian. Note that $|A_4| = 12 = 2^2 \cdots 3$. If there exists $N \trianglelefteq A_4$...

Finish it!

---

8This problem appears, for example, in Hungerford [2], p. 107.
9Note that we could have used the series $(e) \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ to prove that $S_4$ is solvable, and in this case the factor groups are not all cyclic, since $V_4/(e) \cong \mathbb{Z_2} \oplus \mathbb{Z_2}$ is not one-generated.
2. List all abelian groups of order 100. Prove that your list is complete.

Solution: Since \(100 = 2^2 \cdot 5^2\), the (isomorphism classes of) abelian groups of order 100 are

\[
\begin{align*}
Z_2 \oplus Z_5^2 & \cong Z_{100} \\
Z_2 \oplus Z_5 \oplus Z_5 & \cong Z_20 \oplus Z_5 \\
Z_2 \oplus Z_2 \oplus Z_5^2 & \cong Z_2 \oplus Z_{50} \\
Z_2 \oplus Z_2 \oplus Z_5 \oplus Z_5 & \cong Z_{10} \oplus Z_{10}.
\end{align*}
\]

This list is complete by the fundamental theorem of finitely generated abelian groups.

Elaborate!

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

Solution: Let \(G\) be a group of order \(|G| = 168 = 2^3 \cdot 3 \cdot 7\). If \(a \in G\) and \(|a| = 7\) then \((a)\) is a subgroup of order 7, and since 7 is the highest power of 7 dividing 168, \((a)\) is a Sylow 7-subgroup of \(G\). We count the number \(n_7\) of Sylow 7-subgroups using the Sylow theorems, which imply

\[
n_7 \equiv 1 \pmod{7} \quad \text{and} \quad n_7 \mid |G : (a)|.
\]

Since \(|G : (a)| = 24\), then \(n_7 \in \{1, 8\}\). If \(n_7 = 1\), then there are only 6 elements of order 7 in \(G\). If \(n_7 = 8\), then, since the Sylow 7-subgroups must intersect at \((e)\), there are \(6 \cdot 8 = 48\) elements of order 7...

Finish it!

4. Let \(G' < G\) be the commutator subgroup of a finite group \(G\). Let \(Z\) be the center of \(G\). Let \(p\) be a prime number. Suppose that \(p\) divides \(|Z|\) but does not divide \(|Z \cap G'|\). Show that \(G\) has a subgroup of index \(p\).

5. Assume \(G\) is a finite group, \(p\) the smallest prime dividing the order of \(G\), and \(H\) a subgroup of index \(p\) in \(G\). Prove that \(H\) is a normal subgroup of \(G\).
2 Ring Theory

2.1 1992 November

1. \(^{10}\) a. Define “injective module.”
   b. Prove: The module $Q$ is injective if every diagram with exact row

$$
0 \rightarrow P' \rightarrow P \\
\phi \downarrow \quad Q
$$

with projective $P$ is embeddable in a commutative diagram

$$
0 \rightarrow P' \rightarrow P \\
\phi \downarrow \quad Q
$$

2. Let $R$ be a commutative ring with identity. Recall that an ideal $P \subset R$ is said to be prime if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$. Let $J \subseteq R$ be an ideal.
   a. Show that $J$ is prime if and only if $R/J$ is an integral domain.
   b. Show that $J$ is maximal if and only if $R/J$ is a field.

Solution: This is problem 2 of the April 2008 exam. (See section 2.10 below.)

3. Let $R$ be a principal ideal domain. Let $J_1, J_2, \ldots$ be ideals in $R$ such that

$$
J_1 \subseteq J_2 \subseteq \cdots \subseteq J_i \subseteq J_{i+1} \subseteq \cdots
$$

Show that there is an integer $n \geq 1$ such that $J_i = J_n$ for all $i \geq n$.

Solution: This is simply the statement that a PID is Noetherian. It is proved as follows: Let $J = \bigcup J_i$ and check that $J$ is an ideal of $R$. Since $R$ is a PID, $J$ is principal, or “one-generated.” That is, $J = Ra$ for some $a \in R$. Now $a \in Ra = \bigcup J_i$ implies $a \in J_n$ for some $n \in \mathbb{N}$. Therefore, as $Ra$ is the smallest ideal containing $a$, we have $Ra \subseteq J_n \subseteq \bigcup J_i = Ra$, and similarly for all $J_i$ with $i \geq n$. \(\square\)

4. Let $R$ be a ring and $M$ a (left) $R$-module. Suppose $M = K \oplus L$ and $\varphi$ is an $R$-endomorphism of $M$ with the property that $\varphi(L) \subseteq K$. Prove that $M = K \oplus (1_M + \varphi)(L)$.

\(^{10}\)Part b. of this problem makes no sense to me. If it makes sense to you, please email me! williamdemeo@gmail.com
2.1 1992 November  

RING THEORY

5. Let $R$ be any ring, $M, N, K$ submodules of some $R$-module such that $N \leq M$. Prove that the sequence

$$0 \rightarrow \frac{M \cap K}{N \cap K} \rightarrow \frac{M}{N} \rightarrow \frac{M + K}{N + K} \rightarrow 0$$

is exact where the maps are the natural (obvious) ones.

**Solution:** The natural maps are

$$f : \frac{M \cap K}{N \cap K} \ni x \mapsto x + N \in M/N$$

and

$$g : \frac{M}{N} \ni x + N \mapsto x + (N + K) \in \frac{M + K}{N + K}.$$  

It is easy to check that these are well-defined homomorphisms. To see that $f$ is injective, consider

$$\ker(f) = \{x + (N \cap K)| x \in M \cap K \text{ and } x + N = 0\} = \{x + (N \cap K)| x \in N \cap K\} = \{0\},$$

where the first 0 denotes $N$ (the zero of $M/N$), while the second 0 denotes $N \cap K$ (the zero of $\frac{M \cap K}{N \cap K}$). To see that $g$ is surjective, consider $\text{im}(g) = \{x + (N + K)| x \in M\} = M/(N + K)$, and note that $x + (N + K) = x + y + (N + K)$ for any $y \in K$, so $M/(N + K) = (M + K)/(N + K)$.

It remains to show that $\text{im}(f) = \ker(g)$, and, as we see below, this turns out to be equivalent to

**The Modular Law.**  

If $N, M, K$ are submodules of some module, and $N \leq M$, then

$$M \cap (N + K) = N + (M \cap K).$$  

(2)

This law is easy to prove by checking both inclusions; that is, consider an element of each side of (2) and show it is contained in the other side.

Finally, observe,

$$\ker(g) = \{x + N \in M/N| x \in N + K\} = \{x + N| x \in M \text{ and } x \in N + K\}$$

$$= \{x + N| x \in M \cap (N + K)\} = \{x + N| x \in N + (M \cap K)\} \quad \text{(the modular law)}$$

$$= \{x + N| x \in M \cap K\} = \text{im}(f).$$

\[\square\]

---

11 I write $1_M - \varphi$ instead of $1_M + \varphi$ because the former seems a bit more natural to me, but it makes no real difference.

12 See Kasch and Mader [4], page 4, or better yet, work out the details over dinner.

13 In lattice theory, we say that a lattice is **modular** if it satisfies the **modular law**: for elements $a, b, c$ of the lattice, if $a \leq b$, then $b \land (a \lor c) = a \lor (b \land c)$. Not coincidentally, the lattice of submodules of a module satisfies the modular law (where join is $+$ and meet is $\cap$). Alas, mathematical terminology is not always perverse!
Remark: The modular law is sometimes called the Dedekind identity. This identity, and its consequence, \( \text{im}(f) = \ker(g) \), is the crux of problem 5. In fact, Kasch and Mader ([4], page 5) call the exact sequence

\[
\begin{align*}
0 & \to M \cap K \\
& \to N \cap K \\
& \to M + K \\
& \to N + K \\
& \to 0
\end{align*}
\]

"a useful and attractive version of the Dedekind identity."

6. Let \( F \) be a field and let \( R = F(X,Y) \) be the polynomial ring over \( F \) in indeterminates \( X,Y \). Let \( \alpha, \beta \in F \), and let \( \varphi : R \to F \) be defined by \( \varphi(f(X,Y)) = f(\alpha, \beta) \) for all polynomials \( f(X,Y) \in R \). Show that \( \ker(\varphi) = (x - \alpha, y - \beta) \).

7. Let \( R \) be a ring which is generated (as a (left) \( R \)-module) by its minimal left ideals (i.e., \( R \) is semi-simple).
   a. Prove that \( R \) is the direct sum of a finite number of minimal left ideals.
   b. Prove that every simple \( R \)-module is isomorphic to a left ideal of \( R \).

Solution: a. Assume the left regular \( R \)-module, \( R_R \), is semi-simple, by which we mean here that

\[
R = \bigoplus_{i \in I} A_i
\]

for some collection \( \{A_i|i \in I\} \) of minimal left ideals of \( R \). We assume that all rings are unital, so \( 1 \in R \). Note that, although the direct sum (3) may be infinite, each \( r \in R \) is a sum of finitely many elements from the set \( \bigcup\{A_i|i \in I\} \). In particular, \( 1 = a_{i_1} + \cdots + a_{i_n} \) for some finite collection of indices \( \{i_1, \ldots, i_n\} \subseteq I \) and \( a_{i_j} \in A_{i_j} \). Therefore,

\[
R = R1 = R(a_{i_1} + \cdots + a_{i_n}) \subseteq \bigoplus_{j=1}^n A_{i_j} \subseteq \bigoplus_{i \in I} A_i = R,
\]

which proves that \( R \) is the finite direct sum \( \bigoplus_{j=1}^n A_{i_j} \). \( \square \)

8. Let \( R \) be a commutative ring. Prove that an element of \( R \) is nilpotent if and only if it belongs to every prime ideal of \( R \).

Solution: If \( s \in R \) is nilpotent, then \( s^n = 0 \) for some \( n \in \mathbb{N} \). In particular, \( s^n = 0 \in P \) for any ideal \( P \) of \( R \). If \( P \) is prime, then \( s^n \in P \) implies \( s \in P \).

To prove the converse, recall the following useful theorem:\textsuperscript{14}

Theorem: If \( S \) is a multiplicative subset of a ring \( R \) which is disjoint from an ideal \( I \) of \( R \), then there exists an ideal \( P \) which is maximal in the set of all ideals \( R \) disjoint from \( S \) and containing \( I \). Furthermore, any such ideal \( P \) is prime.

If \( s \in R \) is not nilpotent, consider the set \( S = \{s, s^2, s^3, \ldots\} \). Clearly this is a multiplicative set which is disjoint from the ideal \((0)\). The theorem then gives a prime ideal \( P \) disjoint from \( S \). In particular, \( s \notin P \). \( \square \)

(See also April ’08 (2d.).)

\textsuperscript{14}This is proved in the appendix; see Theorem A.2.
2.2 1995 April

1.\(^{15}\) Let \(R\) be a commutative ring. Recall that the annihilator of an element \(x\) in an \(R\)-module is the ideal \(\text{ann}(x) = \{s \in R : sx = 0\}\). Let \(Rx\) and \(Ry\) be cyclic \(R\)-modules.

   a. Show that \(Rx \otimes_R Ry = R(x \otimes y)\).
   b. Show that \(R(x \otimes y) \cong R/(\text{ann}(x) + \text{ann}(y))\).
   c. Show that \(\text{ann}(x \otimes y) = \text{ann}(x) + \text{ann}(y)\).

2.\(^{16}\) Let \(R\) be a ring and suppose that \(I, J\) are left ideals of \(R\) such that \(I + J = R\). Prove that

\[
\frac{R}{I \cap J} \cong \frac{R}{I} \oplus \frac{R}{J}.
\]

3.\(^{17}\) Recall that an ideal \(I\) of a ring \(R\) is nilpotent if \(I^n = 0\) for some positive integer \(n\).

   a. Show: If \(I\) and \(J\) are nilpotent ideals, then so is \(I + J\).
   b. Let \(R = \mathbb{Q}[X, Y]/(X^2, Y^2)\). Show that \(R\) contains a unique largest nilpotent ideal and find it.

4. The **injectivity class** of an \(R\)-module \(C\) is defined to be the class \(\text{Inj}(C)\) consisting of all modules \(B\) such that for every submodule \(A\) of \(B\), every \(R\)-homomorphism \(h : A \to C\) extends to a homomorphism \(h' : B \to C\). Prove that the injectivity class of \(C\) is closed under epimorphic images; i.e., if \(B \in \text{Inj}(C)\) and \(f : B \to B'\) is an epimorphism, then \(B' \in \text{Inj}(C)\).

5.\(^{18}\) Let \(M\) and \(N\) be finitely generated modules over the polynomial ring \(\mathbb{Q}[x]\). Show that \(M\) and \(N\) are isomorphic if \(M\) is isomorphic to a direct summand of \(N\) and \(N\) is isomorphic to a direct summand of \(M\).

---

15 See also November ’99, problem 4.
16 See also November ’95, problem 4.
17 See also November ’97, problem 5.
18 See also November ’97, problem 2.
Instructions: Ph.D. students should attempt at least three problems, M.A. students should attempt at least two.

It goes without saying that all rings have an identity. Integral domains are commutative, other rings are not necessarily commutative unless so specified.

1. Recall that an element \( r \) in an integral domain \( R \) is called irreducible if whenever \( r = ab \) for \( a, b \in R \), then either \( a \) or \( b \) must have an inverse.\(^{19}\)
   a. Prove that an element \( r \) is irreducible if and only if \( (r) \) is maximal among principal ideals; i.e., \( (r) \) is not properly contained in any other principal ideal.
   b. Prove that a Noetherian integral domain \( R \) is a unique factorization domain if and only if all principal ideals generated by irreducible elements are prime.

2. Let \( R \) be a unique factorization domain. A polynomial \( f \in R[X] \) is called primitive if \( f \notin aR[X] \) for any proper ideal \( a \) of \( R \).
   a. Prove that a polynomial \( f \) is primitive if and only if \( f \notin pR[X] \) for any prime ideal \( p \) of \( R \).
   b. Prove that the product of two primitive polynomials is primitive. (This is essentially Gauss’s Lemma.)
   c. Show, in outline, how to use Gauss’s Lemma to prove that the polynomial ring \( R[X] \) is a unique factorization domain.

3. Prove that an integral domain \( R \) has the property that every submodule of a free \( R \)-module is free if and only if \( R \) is a principal ideal domain.

4. Let \( I \) and \( J \) be ideals in a commutative ring \( R \) such that \( I + J = R \).
   a. Prove that \( IJ = I \cap J \).
   b. Prove that \( R/IJ \cong R/I \oplus R/J \).
   c. Prove that \( I \oplus J \cong R \oplus IJ \).

5. a. Prove that a ring \( R \) is left Noetherian if and only if all submodules of finitely generated left \( R \)-modules are finitely generated.
   b. Prove that over any ring, a direct summand of a finitely generated module is finitely generated. (I.e., if \( M \oplus N \) is finitely generated, then \( M \) is finitely generated.)
   c. Prove that over any ring \( R \), a module is finitely generated and projective if and only if it is isomorphic to a direct summand of a free \( R \)-module with finite rank (i.e., of the form \( R^n \) for some finite \( n \)).

6. Let \( M \) be a module over a commutative ring \( R \). Let \( p \) be a prime ideal in \( R \) and let \( M_p \) be the localization of \( M \) at \( p \).
   a. Prove that for \( m \in M, 0 \neq \frac{n}{1} \in M_p \) if and only if \( \operatorname{ann}(m) \subseteq p \), where \( \operatorname{ann}(m) = \{ r \in R \mid rm = 0 \} \).
   b. Prove that an \( R \)-module \( M \) is non-trivial if and only if \( M_m \neq 0 \) for some maximal ideal \( m \) of \( R \).

\(^{19}\) Actually, that’s not quite the right definition – we should also assume \( r \) is a nonzero nonunit element of \( R \).
2.4 1996 April

1. Identify the following rings (integral domain, unique factorization domain, principal ideal domain, Dedekind domain, Euclidean domain, etc), citing theorems to justify your answers and giving examples to show why it is not of a more specialized class.

   a. \( \mathbb{F}_2[x, y] \)
   b. \( \mathbb{F}_2[x, y]/(y^2 + y + 1) \)
   c. \( \mathbb{R}[x, y]/(x^2 + y^2) \)
   d. \( \mathbb{C}[x, y]/(x^2 + y^2) \)
   e. \( \mathbb{Z}[(\sqrt{-5})] \)

Solution:

Lemma: If \( D \) is an integral domain containing an irreducible element \( c \in D \), then \( D[x] \) is not a PID.

Proof: Let \( c \) be an irreducible element in \( D \) (i.e. \( c \) is a nonzero nonunit and \( c = ab \) only if \( a \) or \( b \) is a unit). Suppose \( D[x] \) is a PID, and consider the ideal \((c, x)\) of \( D[x] \). Then \((d) = (c, x)\) for some \( d \in D[x] \). This implies \( c \in (d) \), so \( c = gd \), for some \( g \in D[x] \). By irreducibility of \( c \), either \( g \) is a unit or \( d \) is a unit. If \( d \) is a unit, then \((d)\) would be all of \( D[x] \). But \((d) = (c, x) \neq D[x] \) (for one thing, \( 1 \notin (c, x) \)), so \( d \) is not a unit. Therefore, \( g \) must be a unit, so we can write \( d = g^{-1}c \). This implies \( d \in (c) \), so \((c, x) = (d) = (c) \). It follows that \( x \in (c) \), and thus \( x = fc \) for some \( f \in D[x] \). Finally, \( x \) is irreducible, so \( f \) must be a unit, but this puts both \( f \) and \( c \), hence \( x \), in \( D \), which is impossible.

\( \square \)

Corollary 2.1 If \( \mathbb{F} \) is a field and \( n \geq 2 \), then \( \mathbb{F}[x_1, \ldots, x_n] \) is not a PID.

This follows from the lemma above since \( x_1 \) is irreducible in \( \mathbb{F}[x_1, \ldots, x_n] \). (If \( x_1 = ab \) for some \( a, b \in \mathbb{F}[x_1, \ldots, x_n] \), then, arguing by degree, either \( a \in \mathbb{F} \) or \( b \in \mathbb{F} \).)

Theorem 2.1 If \( D \) is a UFD, then so is the polynomial ring \( D[x_1, \ldots, x_n] \).

By corollary 2.1 above, however, \( D[x_1, \ldots, x_n] \) need not be a PID when \( n \geq 2 \). (Note that a field is trivially a UFD.)

a. \( \mathbb{F}_2[x, y] \)

   Since \( \mathbb{F}_2 \) is a field, it is a UFD, so theorem 2.1 implies that \( \mathbb{F}_2[x, y] \) is a UFD. However, as in the corollary above, \( \mathbb{F}_2[x, y] \) is not a PID. In particular, \((x, y)\) is a (maximal) ideal in \( \mathbb{F}_2[x, y] \) which is not principal, as the reader may easily verify.

b. \( \mathbb{F}_2[x, y]/(y^2 + y + 1) \)

   Letting \( D = \mathbb{F}_2[x] \), we have \( \mathbb{F}_2[x, y]/(y^2 + y + 1) = D[y]/(y^2 + y + 1) \). It is easily verified that \( D \) is a Euclidean domain with norm \( \phi(f) = \deg(f) \). Now, if the polynomial \( g(y) = y^2 + y + 1 \) is irreducible in \( D[y] \), then \((g(y))\) is a maximal ideal and so \( D[y]/(g(y)) \) is a field. To show that \( g(y) \) is, indeed, irreducible, suppose \( g(y) = ab \), for some \( a, b \in D[y] \). Then \( \deg_a(a) = \deg_{xy}(b) = 0 \) so \( a, b \in \mathbb{F}_2[y] \). If they are to be nonunits, \( a \) and \( b \) must have \( \deg_a(a) = \deg_{xy}(b) = 1 \). The only choices are \( a = y - \alpha \) and \( b = y - \beta \) for some \( \alpha, \beta \in \mathbb{F}_2 \). That is, \( g(y) = y^2 + y + 1 \) must have roots in \( \mathbb{F}_2 \), which it does not (\( g(0) = 1 \) and \( g(1) = 3 \equiv 1 \)). Therefore, \( g(y) \) is irreducible in \( D[y] = \mathbb{F}_2[x, y] \). We have thus shown that \( E = \mathbb{F}_2[x, y]/(y^2 + y + 1) \) is a field.

---

20 This is Exercise III.6.1 of Hungerford [2], page 165.
21 To see that \( x \) is irreducible in \( D[x] \), argue by degree.
c. \( \mathbb{R}[x, y]/(x^2 + y^2) \)

First note that \((x^2 + y^2)\) is not a maximal ideal of \( \mathbb{R}[x, y] \). For, \((x^2 + y^2) \subsetneq (x, y) \subseteq \mathbb{R}[x, y] \). Letting \( D = \mathbb{R}[x] \), and \( p(y) = x^2 + y^2 \), we have \( \mathbb{R}[x, y]/(x^2 + y^2) = D[y]/(p(y)) \). The roots of \( p(y) \) are \( \pm \sqrt{-1}x \) which do not belong to \( D \). Thus \( p(y) \) is irreducible in \( D[y] \). What else can we say about \( \mathbb{R}[x, y]/(x^2 + y^2) = D[y]/(p(y)) \)?

Finish this one!

d. \( \mathbb{C}[x, y]/(x^2 + y^2) \)

Let \( D = \mathbb{C}[x] \) and consider \( \mathbb{C}[x, y]/(x^2 + y^2) = D[y]/(p(y)) \), where \( p(y) = x^2 + y^2 \). The roots of \( p(y) \) in \( D[y] = \mathbb{C}[x, y] \) are \( \pm ix \), and so \( p(y) \) factors in \( \mathbb{C}[x, y] \) as \( x^2 + y^2 = (y + ix)(y - ix) \). Therefore, \( \mathbb{C}[x, y]/(x^2 + y^2) \) has zero divisors: let \( a = y + ix + (x^2 + y^2) \) and \( b = y - ix + (x^2 + y^2) \). Then \( ab = (x^2 + y^2) = 0 \in \mathbb{C}[x, y]/(x^2 + y^2) \). Therefore, \( \mathbb{C}[x, y]/(x^2 + y^2) \) is not a domain.

e. \( \mathbb{Z}[\sqrt{-5}] \)

This is a domain (as a subring of \( \mathbb{C} \)) which is not a UFD. For example, \( 9 \) has a non-unique factorization as a product of irreducibles:

\[
9 = 3 \cdot 3 = (2 + \sqrt{5}) \cdot (2 - \sqrt{5}).
\]

Some useful references for problem 1 are Hungerford [2] (in particular, p. 139 and cor. 6.4, p. 159), and Jacobson [3] (p. 141).

2. a. Describe the ring \( \mathbb{Q} \otimes_\mathbb{Z} \mathbb{Q} \).

b. Generalize the result of part a. to \( \mathbb{Q} \otimes_\mathbb{Z} A \), where \( A \) is a divisible abelian group. Note: the group \( A \) (written additively) is called divisible if for any integer \( n \geq 2 \) and any element \( a \in A \), there exists an element \( b \in A \) such that \( nb = a \).

c. A ring as in b. is called a local ring. Show that a commutative ring is local if and only if the set of nonunits forms an ideal.

Solution: a. Let \( \mathcal{J} \) be the set of all proper ideals in \( R \) and consider the partially ordered set \((\mathcal{J}, \subseteq)\). Let \( \{A_\alpha : \alpha \in \mathcal{A}\} \) be any chain in \( \mathcal{J} \) - i.e. \( \mathcal{A} \) is a totally ordered index set and for all \( \alpha, \beta \in \mathcal{A} \), if \( \alpha \leq \beta \), then \( A_\alpha \subseteq A_\beta \). Define \( J = \bigcup_{\alpha \in \mathcal{A}} A_\alpha \). We verify that \( J \) is a proper ideal of \( R \). Of course, as a union of subgroups of the abelian group \( \langle R; +, 0 \rangle \), \( J \) is a subgroup. Fix \( r \in R \) and \( j \in J \). Then there exists \( A_\alpha \in \mathcal{J} \) such that \( j \in A_\alpha \), so \( rj \in A_\alpha \subseteq J \). Therefore, \( J \) is an ideal. It is a proper ideal because otherwise \( 1_R \in J \), which would imply that \( 1_R \in A_\alpha \) for some \( \alpha \in \mathcal{A} \). But then \( A_\alpha = R \) which contradicts the definition of \( \mathcal{J} \).

28
Thus, we have $J \in \mathcal{J}$, and $J$ is an upper bound for $\{A_\alpha : \alpha \in \mathcal{A}\}$. By Zorn’s lemma, $\mathcal{J}$ has a maximal element.

b. For an example of a commutative ring with only one maximal ideal, take the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and define $+$ and $\cdot$ on $\mathbb{Z}_4$ to be addition mod 4 and multiplication mod 4, respectively. Then the ideal generated by 2 is $(2) = \{0, 2\}$, and this is the only maximal ideal. For 1 and 3 are units, so $(1) = (3) = \mathbb{Z}_4$. (You should generalize this argument and convince yourself that, if $p$ is prime and $n \geq 1$, then $\mathbb{Z}_{p^n}$ is a ring with unique maximal ideal $(p)$.)

c. A ring is called a local ring iff it has a unique maximal ideal. Let $R$ be a commutative ring with $1_R$. We must show that $R$ is local iff the set of nonunits forms an ideal. To do so, we prove the equivalence of the following three statements:

(i) $R$ is a local ring.
(ii) All nonunits of $R$ are contained in some ideal $M \neq R$.
(iii) The set of all nonunits of $R$ forms an ideal.

Throughout, we let $S$ denote the set of all nonunits in $R$. We will prove (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii).

Suppose (ii) holds so that $S \subseteq M$ where $M$ is a proper ideal of $R$. Of course, an ideal is a proper ideal iff it contains only nonunits. Therefore, $S \subseteq M \subseteq S$, so $S = M$, which proves (iii).

Suppose (iii) holds, and let $S \subseteq J \subseteq R$ be a chain of ideals. Then, as above, $J = R$ unless $J \subseteq S$, so $S$ contains all proper ideals of $R$. By (iii), $S$ itself is an ideal, so it is the unique maximal ideal, which proves (i).

If (i), then there is a unique maximal ideal $M \subseteq R$. Fix $a \in S$. Now, there is always a maximal ideal of $R$ which contains the ideal $(a)$ (by Zorn’s lemma). But $M$ is the unique maximal ideal of $R$. Therefore, $(a) \subseteq M$. Since $a \in S$ was arbitrary, this proves that $S \subseteq M$ and (ii) holds.

4. a. Let $R$ be a commutative ring and $M$ an $R$-module. Show that $\text{Hom}_R(R, M)$ and $M$ are isomorphic as left $R$-modules.

b. It is clear that $\text{Hom}_R(R, M) \subseteq \text{Hom}_\mathbb{Z}(R, M)$. Give an explicit example of a $\mathbb{Z}$-module homomorphism which is not an $R$-module homomorphism.

5. Let $M$ be a module over an arbitrary ring $R$.

a. Define what it means for $M$ to be projective.

b. Prove that $M$ is projective if and only if it is a direct summand of a free $R$-module.
2.5 1999 March

Instructions: Do as many problems as you can. You are not expected to do all of the problems; you should try to have a collection of solutions balanced among the sections. You may use earlier parts of a problem to solve later parts, even if you cannot solve the earlier part. Most importantly, give careful solutions.

Ph.D. candidates should not do the starred problems.

1. * Suppose $D$ is a commutative ring (not necessarily with 1) having no zero divisors. Give a definite construction of a field in which $D$ can be embedded along with the embedding. You don’t need to prove anything beyond that the operations are well defined and that the set of your construction is closed under the operations.

2. a. Every Euclidean domain is a principal ideal domain.
   b. Every principal ideal domain satisfies the ascending chain condition for ideals.
   c. Give an example of a unique factorization domain that is not a principal ideal domain.

3. Any finitely generated module over a principal ideal domain is the direct sum of its torsion submodule and a free module.

4. Suppose $R$ is a ring.
   a. Suppose $A$ is a right $R$-module and $B$ is a left $R$-module. Define the Abelian group $A \otimes R B$.
   b. Show that $A \otimes_R R$ and $A$ are isomorphic Abelian groups.

5. Let $I$ be an infinite set. Suppose for each $i \in I$ that $F_i$ is a field. $\prod (F_i : i \in I)$ denotes the direct product of the family of fields, and $\sum (F_i : i \in I)$ denotes the direct sum, and the latter set consists of those sequences belonging to the direct product that have 0 in all but finitely many places. Show that the ring $\prod (F_i : i \in I) / \sum (F_i : i \in I)$ has a homomorphic image which is a field. (Any assertion you make about the existence of an ideal should be proved.)
2.6 2003 April

1. Let $R$ be a ring, $I$ a right ideal and $J$ a left ideal of $R$. The expression $I + J$ stands for the Abelian group generated by $I \cup J$. Prove that

\[ \frac{R}{I} \otimes_R \frac{R}{J} \cong \frac{R}{I + J}. \]

Define your maps carefully with particular attention to well-definedness.

Solution:

**Lemma 2.1** Every element of $\frac{R}{I} \otimes_R \frac{R}{J}$ can be written as a simple tensor $(1 + I) \otimes (r + J)$, for some $r \in R$.

Note that every element can certainly be written as a finite sum of generators, say, $(s_1 + I) \otimes (r_1 + J) + \cdots + (s_n + I) \otimes (r_n + J)$. Also, $(s_1 + I) \otimes (r_1 + J) = (1 + I) \otimes (s_1 r_1 + J)$, so

\[ \sum_{i=1}^{n} (s_i + I) \otimes (r_i + J) = \sum_{i=1}^{n} (1 + I) \otimes (s_i r_i + J) = (1 + I) \otimes \left( \sum_{i=1}^{n} s_i r_i \right) + J. \]

This proves the lemma.

Now define the map $\theta : \frac{R}{I} \times \frac{R}{J} \to \frac{R}{I + J}$ by $\theta(s + I, r + J) = sr + (I + J).$ This is clearly a well-defined mapping from one abelian group to another. For, if $(s + I, r + J) = (s' + I, r' + J)$, then $s - s' \in I$ and $r - r' \in J$.

\[ sr - s' r' = sr - sr' + sr' - s' r' = s(r - r') + (s - s') r' \in I + J. \]

Therefore, $(s + I, r + J) = (s' + I, r' + J)$ implies $\theta(s + I, r + J) = \theta(s' + I, r' + J)$.

A routine calculation shows that the mapping $\theta$ is bilinear, and therefore (by the universal property of tensor products) induces a unique homomorphism $\hat{\theta} : \frac{R}{I} \otimes_R \frac{R}{J} \to \frac{R}{I + J}$, which is clearly surjective. To show that $\hat{\theta}$ is also injective, suppose $x \in \ker \hat{\theta}$. By lemma 2.1, $x = (1 + I) \otimes (r + J)$ for some $r \in R$, and

\[ 0 = \hat{\theta}(x) = r + (I + J) \Rightarrow r \in I + J \Rightarrow r = i + j, \]

for some $i \in I$ and $j \in J$. Therefore,

\[ x = (1 + I) \otimes (i + j + J) = (1 + I) \otimes (i + J) = (i + I) \otimes (1 + J) = I \otimes (1 + J) = 0. \]

This shows that $\ker \hat{\theta} = 0$, so $\hat{\theta}$ is an isomorphism.

2. a. Let $A_1$ and $A_2$ be modules over some ring, $K_1 \subseteq A_1$ and $K_2 \subseteq A_2$ be submodules, and $\gamma_1 : A_1 \to A_2$ and $\gamma_2 : A_2 \to A_1$ be homomorphisms with the following properties.

i. $\gamma_1(K_1) \subseteq K_2$ and $\gamma_2(K_2) \subseteq K_1$, and

ii. $(1 - \gamma_2 \gamma_1)(A_1) \subseteq K_1$ and $(1 - \gamma_1 \gamma_2)(A_2) \subseteq K_2$.

Show that the maps

\[ f : A_1 \oplus K_2 \to A_2 \oplus K_1 : f((x_1, y_2)) = (\gamma_1(x_1) - y_2, -x_1 + \gamma_2 \gamma_1(x_1) - \gamma_2(y_2)) \]

and

\[ g : A_2 \oplus K_1 \to A_1 \oplus K_2 : g((x_2, y_1)) = (\gamma_2(x_2) - y_1, -x_2 + \gamma_1 \gamma_2(x_2) - \gamma_1(y_1)) \]

are well-defined homomorphisms and that $g = f^{-1}$. 

31
b. Let $P_1$ and $P_2$ be projective modules and $M$ a module over some ring $R$. Suppose that $\beta_1 : P_1 \to M$ and $\beta_2 : P_2 \to M$ are epimorphisms. Show that

$$P_1 \oplus \ker(\beta_2) \cong P_2 \oplus \ker(\beta_1).$$

3. Let $M_n(R)$ be the ring of matrices with coefficients in a ring $R$ (with 1), where $n$ is a natural number > 1. For a (two-sided) ideal $I$ of $R$, let

$$M_n(I) = \{[a_{ij}] \in M_n(R) : a_{ij} \in I\}.$$

a. Prove that $M_n(I)$ is an ideal of $M_n(R)$.

b. Prove that every ideal of $M_n(R)$ is of the form $M_n(I)$ for a suitable ideal $I$ of $R$.

Solution: The first part is very easy. The second part is proved for $n = 2$ below (see proposition A.1), and for the general case in Lam’s book [5].

4. Recall that a module is simple if it is nontrivial and has no proper submodules.

a. Prove that the endomorphism ring of a simple module is a division ring (= skew field).

b. Prove that a ring $R$ with identity 1 contains a left ideal $I$ such that $R/I$ is a simple left $R$-module.

c. Let $R$ be a ring with identity 1 and suppose that $M = \_R M$ is a left $R$-module with the property that every submodule is a direct summand (“everybody splits”). Show that every non-zero submodule $K$ of $M$ contains a simple submodule.

Solution: a. Let $M$ be a simple $R$-module, and suppose $\varphi$ is an endomorphism of $M$ that is not identically zero. We must show that $\varphi$ is invertible. It suffices to show that $\varphi$ is injective. $M$ is simple, so $\{0\}$ and $M$ are the only submodules. Of course, $\ker \varphi$ and $\text{im} \varphi$ are both submodules of $M$ (as is easily verified). Since $\varphi$ is not the zero map, it must be the case that $\text{im} \varphi \neq \{0\}$ and $\ker \varphi \neq M$. Thus, $\varphi$ is bijective.

b. By the standard Zorn’s lemma argument, we can find a maximal left ideal $I$ in $R$. It is easily verified that $R/I$ is a left $R$-module. Suppose $M$ is a left $R$-submodule of $R/I$. Then, in particular, $M$ is a left ideal of $R/I$. Recall that the left ideals of $R/I$ are in one-to-one correspondence with the left ideals of $R$ which contain $I$. Moreover, each left ideal in $R/I$ has the form $J/I$ for some left ideal $J$ in $R$ containing $I$ (see, e.g., Hungerford [2], p. 126). Thus, we have a chain of left ideals $I \subseteq J \subseteq R$ with $M = J/I$. Since $I$ is maximal, either $J = I$, in which case $M$ is the zero submodule of $R/I$, or $J = R$, in which case $M = R/I$. Since $M$ was an arbitrary submodule of $R/I$, this proves that $R/I$ is a simple module.

c. Let $k$ be a nonzero element of $K$. Clearly $Rk \subseteq K$ is also a submodule of $M$. Therefore, $M = Rk \oplus N$ for some submodule $N$ of $M$. 

32
2.7 2003 November

1. Let $R$ be a commutative ring, and let $N$ be the set of all nilpotent elements of $R$. Prove that
   a. $N$ is an ideal of $R$, and
   b. $R/N$ has no nonzero nilpotent elements.

2. a. Show that $\mathbb{Z}[\sqrt{-1}]$ is a unique factorization domain (UFD).
   b. Show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Solution:  a. $\mathbb{Z}[\sqrt{-1}]$ can be embedded in $\mathbb{C}$ which is a UFD, so $\mathbb{Z}[\sqrt{-1}]$ is a UFD.
   b. Consider $(a + \sqrt{-3})(a - \sqrt{-3}) = a^2 + 3$. If we let $a = 3$, then
      $$(3 + \sqrt{-3})(3 - \sqrt{-3}) = 12 = 2^2 \cdot 3,$$
      giving two distinct factorizations of $12$ in $\mathbb{Z}[\sqrt{-1}]$. Therefore, $\mathbb{Z}[\sqrt{-1}]$ is not a UFD.

3. Let $R$ be a commutative ring with unit. Show that if $R$ contains an idempotent element $e$, then there exist ideals $S$, $T$ of $R$ such that $R = S \oplus T$.

Solution: Let $\varphi : R \to R$ be defined by $\varphi(r) = er$. Then
$$\varphi(r_1 r_2) = er_1 r_2 = r_1 er_2 = r_1 \varphi(r_2)$$

and
$$\varphi(r_1 + r_2) = e(r_1 + r_2) = er_1 + er_2 = \varphi(r_1) + \varphi(r_2).$$

That is, $\varphi$ is an $R$-module endomorphism (viewing $R$ as a module over itself). Also, $\varphi$ is itself an idempotent element in the ring of endomorphisms $\text{End}_R R$. That is, $\varphi \circ \varphi = \varphi$, as is easily verified.

Let $T = \text{im} \varphi = \{ \varphi(r) : r \in R \}$ and let $S = \ker \varphi = \{ r \in R : \varphi(r) = 0 \}$. Then, for any $r \in R$ we have
$$r = r - \varphi(r) + \varphi(r)$$

with $\varphi(r) \in T$ and, since $\varphi$ is idempotent, $r - \varphi(r) \in S$. Thus $R = S + T$. Now suppose $r \in S \cap T$. Then $r \in T$ implies $r = \varphi(r')$ for some $r' \in R$. On the other hand, $r \in S$ implies $0 = \varphi(r) = \varphi(\varphi(r')) = \varphi(r') = r$, the penultimate equality by idempotence of $\varphi$. This proves that $S \cap T = 0$, so $R = S \oplus T$.

We prove that $S$ and $T$ are ideals by simply checking the required conditions. Fix $s_1, s_2 \in S$, and $r \in R$. First note that $-s_1 \in S$ since $\varphi$ is an $R$-module homomorphism, so $\varphi(-s_1) = \varphi(-1_R s_1) = -1_R \varphi(s_1)$, where $1_R$ is the unit of $R$. It then follows that
$$\varphi(s_1 - s_2) = \varphi(s_1) - \varphi(s_2) = 0 - 0 = 0$$

so $s_1 - s_2 \in S$, which proves that $S$ is a subgroup of the abelian group reduct $\langle R, +, -, 0 \rangle$ of $R$. Finally $\varphi(rs_1) = r \varphi(s_1) = r \cdot 0 = 0$, so $rs_1 \in S$, which proves that $S$ is an ideal.

The proof that $T$ is an ideal is similar; we verify that $T$ is a subgroup of the abelian group reduct $\langle R, +, -, 0 \rangle$, and then check that $rt \in T$ whenever $r \in R$ and $t \in T$.  

□
4. Prove that if $R$ is a commutative ring and $I, J$ are ideals of $R$, then there is an $R$-module isomorphism

$$R/I \otimes R/J \cong R/(I + J).$$

**Solution:** This is the special case (in which $R$ is commutative) of problem 1 of April 2003.

5. Let $M$ be a left $R$-module and $x \in M$. Let $\text{ann}(x) = \{ r \in R : rx = 0 \}$.

   a. Show that $\text{ann}(x)$ is a left ideal of $R$.

   b. Prove that there is an $R$-module isomorphism $Rx \cong R/\text{ann}(x)$.

**Solution:**

   a. Fix $r_1, r_2 \in \text{ann}(x)$ and $r \in R$. Then $(r_1 - r_2)x = r_1x - r_2x = 0$ so $r_1 - r_2 \in \text{ann}(x)$ so $\text{ann}(x)$ is a subgroup of the abelian group reduct $\langle R, +, -, 0 \rangle$. Also, $rr_1x = r0 = 0$ so $rr_1 \in \text{ann}(x)$ which proves that $\text{ann}(x)$ is a left ideal of $R$.

   b. Define $\varphi : R \to Rx$ by $\varphi(r) = rx$. Then $\varphi$ is clearly surjective. Also, $\varphi(r_1r_2) = r_1r_2x = r_1\varphi(r_2)$, so $\varphi$ is an $R$-module epimorphism. Finally,

   $$\ker \varphi = \{ r \in R : rx = 0 \} = \text{ann}(x).$$

   Therefore, by the first isomorphism theorem $R/\text{ann}(x) \cong \text{im} \varphi = Rx.$
2.8 2004 November

Notation: \( \mathbb{Z} \) denotes the ring of integers and \( \mathbb{Q} \) denotes the field of rational numbers.

1. Let \( R \) be a commutative ring.
   
   a. Show that if \( R \) is an integral domain, then the only units in the polynomial ring \( R[x] \) are the units of \( R \).
   
   b. Give counterexamples when \( R \) is not an integral domain,
   
   c. Show that \( R[x] \) is a principal ideal domain if and only if \( R \) is a field.

2. Let \( f \in \mathbb{Z}[x] \) be a monic polynomial of degree \( n \) with distinct roots \( \alpha_1, \ldots, \alpha_r \), \( r \leq n \). Show that \( \alpha_1 + \cdots + \alpha_r \in \mathbb{Z} \).

3. List all the ideals of the quotient ring \( R[x]/I \), where \( I \) is the ideal generated by \((x-5)^2(x^2+1)\). Identify which of the ideals are prime and which are maximal. Does your answer change if the field \( \mathbb{R} \) is replaced by \( \mathbb{C} \)? (Explain.)

4. Let \( M \) be a left module over a ring \( R \).
   
   a. Suppose that \( M \) is finitely generated and that \( R \) is commutative and Noetherian. Sketch a proof that \( M \) is Noetherian; i.e., \( M \) satisfies the ascending chain condition on submodules.
   
   b. Suppose that \( M \) is Noetherian and that \( f : M \to M \) is a surjective homomorphism. Show that \( f \) is an isomorphism.

5. Let \( R \) be a ring with 1 and let \( M \) be an \( R \)-module. Show that the following are equivalent:
   
   a. There exists a module \( N \) such that \( M \oplus N \) is free.
   
   b. Given any surjection \( \varphi : B \to M \), there exists an \( R \)-module homomorphism \( \psi : M \to B \) such that \( \varphi \circ \psi \) is the identity on \( M \).
   
   c. Given a homomorphism \( \varphi : M \to B \) and a surjection \( \pi : A \to B \), there exists a homomorphism \( \psi : M \to A \) such that \( \pi \circ \psi = \varphi \).

6. Let \( R = \mathbb{Z}[i] \) be the ring of Gaussian integers.
   
   a. Show that any nontrivial ideal must contain some positive integer.
   
   b. Find all the units in \( R \).
   
   c. If \( a + bi \) is not a unit, show that \( a^2 + b^2 > 1 \).
1. State a structure theorem for finitely generated modules over a PID, including uniqueness conditions on the direct summands.

**Solution:** If $A$ is a finitely generated module over a PID $R$, then

(i) $A$ is a direct sum of a free submodule $F$ of finite rank and finitely many cyclic torsion modules. The cyclic torsion summands (if any) are of orders $r_1, \ldots, r_t$ where the $r_1, \ldots, r_t$ are (not necessarily distinct) nonzero nonunits in $R$ satisfying $r_1 | r_2 | \cdots | r_t$. The rank of $F$ and the ideals $(r_1), \ldots, (r_t)$ are uniquely determined by $A$.

(ii) $A$ is a direct sum of a free submodule $E$ of finite rank and a finite number of cyclic torsion modules. The cyclic torsion summands (if any) are of orders $p_1^{s_1}, \ldots, p_k^{s_k}$ where the $p_1, \ldots, p_k$ are (not necessarily distinct) primes in $R$ and the $s_1, \ldots, s_k$ are positive integer. The rank of $E$ and the ideals $(p_1^{s_1}), \ldots, (p_k^{s_k})$ are uniquely determined by $A$ (except for the order in which the $p_i$ appear).

Symbolically, the situation in part (i) of this theorem is as follows:

$$A \cong F \oplus Ra_1 \oplus \cdots \oplus Ra_t \cong F \oplus R/(r_1) \oplus \cdots \oplus R/(r_t),$$

where $(r_i) = \text{ann}(a_i) = \{ r \in R : ra_i = 0 \}$. Note that $r_1 | r_2 | \cdots | r_t$ holds if and only if $\text{ann}(a_i) \subseteq \cdots \subseteq \text{ann}(a_1)$, in which case $r_i a_i = 0$ for all $a_i \in \text{Tor}(A)$. The situation in part (ii) of the theorem can be written symbolically as

$$A \cong E \oplus R/(p_1^{s_1}) \oplus \cdots \oplus R/(p_k^{s_k}).$$

2. Suppose that $f : M \to N$ and $g : A \to B$ are homomorphisms of right and left $R$-modules, respectively. Prove that there is a group homomorphism $h : M \otimes_R A \to N \otimes B$ with $h(m \otimes a) = f(m) \otimes g(a)$ for all $a \in A$ and $m \in M$.

3. Let $A$ be an $(R, S)$-bimodule and $B$ be an $(R, T)$-bimodule and let $M = \text{Hom}_R(A, B)$.

a. Give the actions of $S$ and $T$ on $M$ making it an $S$-module and a $T$-module (left or right, as appropriate). No proofs required.

b. Assuming your module actions from the first part, prove that $M$ is in fact an $(S, T)$ or $(T, S)$ bimodule (whichever is appropriate).

**Solution:** a. An action of $S$ on $M$ making $M$ into a left $S$-module is given as follows: for all $s \in S$, $f \mapsto sf$, where $(sf)(a) = f(as)$, for all $a \in A$. An action of $T$ on $M$ making $M$ into a right $T$-module is given as follows: for all $t \in T$, $f \mapsto ft$ where $(ft)(a) = f(a)t$, for all $a \in A$.

b. That $M$ is an $(S, T)$-bimodule can be seen by simply checking that it satisfies the definition; i.e., by checking that $M$ is both a left $S$-module and a right $T$-module. Indeed, for all $a \in A$, $s_1, s_2, s \in S$, $f_1, f_2, f \in M$, we have

$$(s_1 + s_2)f(a) = f(a(s_1 + s_2)) = f(as_1 + as_2) \quad \text{(since $A$ is a right $S$-module)}$$

$$= f(as_1) + f(as_2) = (s_1f)(a) + (s_2f)(a) = (s_1f + s_2f)(a),$$

$$(sf_1 + sf_2)(a) = (f_1 + f_2)(as) = f_1(as) + f_2(as) = sf_1(a) + sf_2(a) = (sf_1 + sf_2)(a),$$

and
and \((s_1(s_2f))(a) = (s_2f)(as_1) = f((as_1)s_2) = f(a(s_1s_2)) = ((s_1s_2)f)(a)\). The penultimate equality holds, again, because \(A\) is a right \(S\)-module. This proves that \(M\) is a left \(S\)-module. The proof that \(M\) is a right \(T\)-module is similar, so we leave it to the reader to check that, since \(B\) is a right \(T\)-module, the following holds:

For all \(a \in A, \ t_1, t_2, t \in T, \ f_1, f_2, f \in M,\)

\[
(f(t_1 + t_2))(a) = (ft_1 + ft_2)(a),
\]

\[
((f_1 + f_2)t)(a) = (f_1t)(a) + (f_2t)(a),
\]

\[
(f(t_1t_2))(a) = ((ft_1)t_2)(a).
\]

It follows that \(M\) is an \((S,T)\)-bimodule. \(\square\)

4. Give an example (no proof required) or prove that none exists:

a. An injective \(\mathbb{Z}[i, \pi]\)-module. (You may assume that \(\pi\) is transcendental over \(\mathbb{Q}\).)

b. A ring which is a UFD but which does not have the ascending chain condition on ideals.

c. Two nonzero \(\mathbb{Q}\)-modules \(M\) and \(N\) with \(M \otimes_{\mathbb{Q}} N = 0\).

d. A Euclidean domain which is not a PID.
2.10 2008 April

1. Let $R$ be a commutative ring.

   a. Define what it means for $R$ to be Noetherian.

   b. Prove that if $R$ is Noetherian, the polynomial ring $R[x]$ is Noetherian.

**Solution:** a. A commutative ring $R$ is Noetherian provided $R$ satisfies the ascending chain condition (ACC) on ideals. That is, for any chain $I_1 \subseteq I_2 \subseteq \cdots$ of ideals of $R$, there is an $N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for all $n \geq N$. (By Zorn’s lemma, a condition which is equivalent to the ACC is that every nonempty set of ideals contains a maximal element.) More generally, an $R$-module is Noetherian provided it satisfies the ACC on submodules.

b. This is the Hilbert Basis Theorem, which can be found in many standard references, for example, Theorem VIII.4.9 of Hungerford [2]. The proof in Hungerford uses a fundamental theorem ([2], VIII.1.9) which is worth noting: a module $M$ is Noetherian if and only if every submodule of $M$ is finitely generated. In particular, a commutative ring $R$ is Noetherian if and only if every ideal of $R$ is finitely generated. Therefore, to show that $R[x]$ is Noetherian, it suffices to show that every ideal $J$ in $R[x]$ is finitely generated.

2. Let $R$ be a commutative ring with identity. Recall that an ideal $P \subset R$ is prime if $P \neq R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$. Let $J \subset R$ be an ideal.

   a. Show that $J$ is prime if and only if $R/J$ is an integral domain.

   b. Show that $J$ is maximal if and only if $R/J$ is a field.

   c. Prove that if $J \neq R$, then $J$ is contained in a maximal ideal.

   d. Prove that an element of $R$ is nilpotent if and only if it belongs to every prime ideal of $R$.

**Solution:** a. First, note that $R/J$ is a commutative ring with multiplication $(a + J)(b + J) = ab + J$, for $a, b \in R$, additive identity $0 = J$, and multiplicative identity $1_R + J$. (That the ring axioms are satisfied is easily verified.)

$(\Rightarrow)$ Suppose $J$ is prime and $(a + J)(b + J) = ab + J = 0 = J$. Then $ab \in J$ so either $a \in J$ and $a + J = 0$ or $b \in J$ and $b + J = 0$. That is, $R/J$ has no zero divisors.

$(\Leftarrow)$ Suppose $R/J$ is an integral domain. Then, since an integral domain has a (non-zero) multiplicative identity – in this case, $1_R + J$ – it’s clear that $J \neq R$. Now, suppose $ab \in J$. Then $(a + J)(b + J) = ab + J = 0$. It follows that either $a + J = 0$ or $b + J = 0$, since $R/J$ is a domain. That is, either $a \in J$ or $b \in J$, which proves that $J$ is prime.

b. $(\Rightarrow)$ Suppose $J$ is maximal and $a + J \neq 0$ in $R/J$. Then $a \notin J$. Consider the ideal generated by $a$ and $J$, denoted $(a, J)$. Since $J \subsetneq (a, J) \subsetneq R$ and $J$ is maximal, it must be the case that $(a, J) = R$. Whence, $1_R \in (a, J)$, so $1_R = ab + rj$ for some $j \in J$, $r, b \in R$. Therefore, $1_R - ab \in J$ so $(a + J)(b + J) = ab + J = 1_R + J$, which shows that $a + J$ is a unit in $R/J$. Since $a + J$ was an arbitrary non-zero element, this proves that $R/J$ is a field.

$(\Leftarrow)$ Suppose $R/J$ is a field. Let $J \subset I \subset R$ be a chain of ideals. Suppose there exists an element $a \in I \setminus J$. Then $a + J$ is non-zero, so there is a $b + J \in R/J$ such that $ab + J = 1_R + J$. Now, since $a \in I$, an ideal, clearly $ab \in I$ as well. Also, $ab - 1_R \in J \subset I$. Therefore, $1_R \in I$, which implies $I = R$. This proves that $J$ is maximal.

c. Let $\mathcal{I}$ be the set of all proper ideals of $R$ which contain $J$. Then $(\mathcal{I}, \subseteq)$ is a partially ordered set. Let $\{J_\alpha : \alpha \in \Lambda\}$ be a chain of subsets of $\mathcal{I}$ indexed by $\Lambda$ (totally ordered by set inclusion). Define $M = \bigcup\{J_\alpha : \alpha \in \Lambda\}$.

---

22This simply means that, for any $\alpha, \beta \in \Lambda$, either $J_\alpha \subset J_\beta$ or $J_\beta \subset J_\alpha$. Consequently, we can totally order the index set $\Lambda$ by declaring $\alpha \preceq \beta$ if and only if $J_\alpha \subseteq J_\beta$.
We verify that (1) $M$ is an ideal and (2) $M$ belongs to $\mathcal{F}$: First, $a, b \in M$ implies $a \in J_\alpha$ and $b \in J_\beta$ for some $\alpha, \beta \in \Lambda$. Without loss of generality, suppose $J_\alpha \subseteq J_\beta$. Then both $a$ and $b$ are in $J_\beta$, so $a - b \in J_\beta \subseteq M$, which proves that $M$ is a subgroup of $(\mathbb{R}, +, 0_R)$. If $r \in \mathbb{R}$, then $ra \in J_\alpha \subseteq M$, so (1) is proved. To see that $M$ is proper, note that $1_R$ cannot belong to $M = \bigcup_\alpha J_\alpha$. For, if $1_R \in M$, then $1_R \in J_\gamma$ for some $\gamma \in \Lambda$. But each $J_\gamma$ is a proper ideal, so this can’t happen. (Any ideal which contains a unit is all of $R$.) We have thus shown that every chain in the poset $(\mathcal{F}, \subseteq)$ has an upper bound in the set $\mathcal{F}$. Therefore, by Zorn’s lemma, $\mathcal{F}$ has a maximal element. That is, $J$ is contained in a maximal ideal. \(\square\)

d. \((\Rightarrow)\) Let $a \in R$ be nilpotent and let $P \subset R$ be a prime ideal. Then $P$ is, in particular, a subgroup of $(\mathbb{R}, +, 0_R)$, so $0_R \in P$. Let $n \in \mathbb{N}$ be such that $a^n = 0_R$. Then $a^n \in P$ and, recall the following fact (Corollary A.1) for prime ideals in a commutative ring: for $b_1, b_2, \ldots, b_k \in R$, if $b_1b_2 \cdots b_k \in P$ then $b_i \in P$ for some $i \in \{1, \ldots, k\}$.

Applied in the present case, $a^n \in P$ implies $a \in P$.

\((\Leftarrow)\) Suppose $a$ is not nilpotent; i.e. for all $n \in \mathbb{N}$, $a^n \neq 0$. Consider the set $A = \{a^n : n \in \mathbb{N}\}$. This is a multiplicative set which is disjoint from the zero ideal $(0)$. By Theorem A.2, then, there is a prime ideal $P$ which is disjoint from $A$, whence $a \notin P$. \(\square\)

(See also November ’92 (6).)

3. Let $R$ be a ring with identity.

a. Suppose that $A$ is a right $R$-module and $B$ is a left $R$-module. Define the abelian group $A \otimes_R B$.

b. Show that $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_d$, where $d = \gcd(m, n)$.

**Solution:** a.\(^{23}\) Let $F$ be the free abelian group on the set $A \times B$ and let $K$ be the subgroup of $F$ generated by all elements of the form

(i) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$
(ii) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$
(iii) $(ar, b) - (a, rb)$

where $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$, and $r \in R$. The quotient group $F/K$ is an abelian group called the tensor product of $A$ and $B$, denoted by $A \otimes_R B$. That is, we define $A \otimes_R B = F/K$.

b. Define the map $\varphi: \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_d$ by $\varphi(x, y) = xy \pmod{d}$, for $x \in \mathbb{Z}_m$, $y \in \mathbb{Z}_n$. Then it is easy to check that $\varphi$ is a middle linear map. That is, $\varphi$ satisfies, for all $x, x_1, x_2 \in \mathbb{Z}_m$, $y, y_1, y_2 \in \mathbb{Z}_n$, and $r \in \mathbb{Z}$,

$$\varphi(x_1 + x_2, y) = \varphi(x_1, y) + \varphi(x_2, y),$$
$$\varphi(x, y_1 + y_2) = \varphi(x, y_1) + \varphi(x, y_2),$$
$$\varphi(xr, y) = \varphi(x, ry).$$

\(^{23}\)In proofs involving Zorn’s lemma, it is often better to use a symbol that signifies an arbitrary index set, like $\Lambda$ (as opposed to, say, $\mathbb{N}$), as we typically want the argument to work for uncountable collections of sets. This may seem like a minor point, but examiners are likely to notice this sort of thing.

\(^{24}\)In my opinion, Hungerford [2] section IV.5, pp. 207–209, gives the clearest, most succinct exposition of the tensor product and its basic properties, and the solution given here reflects this bias.
Therefore, by the universal property, there is a unique (abelian group) homomorphism \( \overline{\varphi} : \mathbb{Z}_m \otimes \mathbb{Z}_n \to \mathbb{Z}_d \) such that \( \overline{\varphi} \iota = \varphi \) where \( \iota \) is the canonical middle linear map, \( (a, b) \mapsto a \otimes b \). In other words, we have the following commutative diagram:

\[
\begin{array}{ccc}
\mathbb{Z}_m \times \mathbb{Z}_n & \xrightarrow{\iota} & \mathbb{Z}_m \otimes \mathbb{Z}_n \\
\pdownarrow{\varphi} & & \pdownarrow{\overline{\varphi}} \\
\mathbb{Z}_d & & \\
\end{array}
\]

The proof is complete if \( \overline{\varphi} \) is actually an isomorphism. Equivalently, there should exist a \( \psi \in \text{Hom}_R(\mathbb{Z}_d, \mathbb{Z}_m \otimes \mathbb{Z}_n) \) such that \( \overline{\varphi} \psi = 1_{\mathbb{Z}_d} \) and \( \psi \overline{\varphi} = 1_{\mathbb{Z}_m \otimes \mathbb{Z}_n} \). Indeed, define \( \psi \) on \( \mathbb{Z}_d \) to be the mapping \( x \mapsto x \otimes 1 \). Then \( \psi \) is a group homomorphism. (Proof: \( \psi(x + y) = (x + y) \otimes 1 = x \otimes 1 + y \otimes 1 = \psi(x) + \psi(y) \) for all \( x, y \in \mathbb{Z}_d \).

Also, for all \( x \in \mathbb{Z}_d \),

\[
\overline{\varphi} \psi(x) = \overline{\varphi}(x \otimes 1) = \overline{\varphi}(x, 1) = \varphi(x, 1) = x1 \mod d = x.
\]

That is, \( \overline{\varphi} \psi = 1_{\mathbb{Z}_d} \). Next consider the action of \( \psi \overline{\varphi} \) on generators of \( \mathbb{Z}_m \otimes \mathbb{Z}_n \): for \( x \in \mathbb{Z}_m, \ y \in \mathbb{Z}_n \),

\[
\psi \overline{\varphi}(x \otimes y) = \varphi(x, y) = \psi(xy \mod d) = xy \mod d \otimes 1 = x \mod d \otimes y \mod d = x \otimes y.
\]

Since \( \psi \overline{\varphi} \) is a homomorphism, the identity (4) extends to finite sums of generators:

\[
\psi \overline{\varphi} \left( \sum_{i=1}^{n} x_i \otimes y_i \right) = \sum_{i=1}^{n} x_i \otimes y_i.
\]

Whence, \( \psi \overline{\varphi} = 1_{\mathbb{Z}_m \otimes \mathbb{Z}_n} \), as desired. \( \square \)
1. List the ideals of the rings:

a. \( \mathbb{Z}/12\mathbb{Z} \)

b. \( M_2(\mathbb{R}) \) (the ring of \( 2 \times 2 \) real matrices)

c. \( \mathbb{Z}/12\mathbb{Z} \times M_2(\mathbb{R}) \).

**Solution:**

a. An ideal is, in particular, a subgroup of the additive group. Since \( (\mathbb{Z}_{12}; +, 0) \) is cyclic, all subgroups are cyclic. Thus, the subgroups of \( (\mathbb{Z}_{12}; +, 0) \) are as follows:

- \( (0) = \{0\} \)
- \( (1) = \{0, 1, \ldots, 11\} \)
- \( (2) = \{0, 2, 4, 6, 8, 10\} \)
- \( (3) = \{0, 3, 6, 9\} \)
- \( (4) = \{0, 4, 8\} \)
- \( (6) = \{0, 6\} \)

Of course, 5, 7, and 11 are relatively prime to 12, so \( (1) = (5) = (7) = (11) = \mathbb{Z}_{12} \). The remaining generators, 8, 4, and 9, are also redundant: \( (8) = (4), (9) = (3), \) and \( (10) = (2) \). It is easy to verify that each of the 6 distinct subgroups listed above – call them \( \{G_i : 1 \leq i \leq 6\} \) – have the property that, if \( r \in \mathbb{Z}_{12} \) and \( a \in G_i \), then \( ra \in G_i \). Thus, each \( G_i, 1 \leq i \leq 6, \) is an ideal of \( \mathbb{Z}_{12} \).

(Remark: This also shows \( \mathbb{Z}_{12} \) is a PID, hence the proper prime ideals are the maximal ideals, \( (2) \) and \( (3) \).)

b. By the following lemma, since \( \mathbb{R} \) is a field (and thus has no non-trivial proper ideals), the only ideals of \( M_2(\mathbb{R}) \) are \( M_2(0) \) and \( M_2(\mathbb{R}) \).

**Lemma 2.2** Let \( R \) be a commutative ring with \( 1_R \neq 0 \). Then the ideals of \( M_2(R) \) are precisely the subsets \( M_2(J) \subseteq M_2(R) \), where \( J \) is an ideal of \( R \).

**Proof:** Suppose \( J \) is an ideal and \( A_1, A_2 \in M_2(J) \). Then \( A_1 - A_2 \) has all elements in \( J \), since \( J \) is, in particular, a subgroup. Therefore \( M_2(J) \) is a subgroup of \( (M_2(R); +, 0) \). If \( M = (m_{ij}) \in M_2(R) \) and \( A = (a_{ij}) \in M_2(J) \), then \( MA = (\sum_{k=1}^2 m_{ik}a_{kj}) \). Clearly, all the elements of \( MA \) are in \( J \), since \( J \) is an ideal and \( a_{ij} \in J \). Similarly, all the elements of \( AM \) are in \( J \). This proves that \( M_2(J) \) is an ideal of \( M_2(R) \) whenever \( J \) is an ideal of \( R \).

Now, let \( \mathcal{I} \subseteq M_2(R) \) be an ideal of \( M_2(R) \), and let \( J \) be the set of all \( a \in R \) such that \( a \) is an element of some \( A \in \mathcal{I} \). Clearly 0 \( \in J \), since \( A \in \mathcal{I} \) implies \( 0 = A - A \in \mathcal{I} \). Let \( a, b \in J \). Suppose \( a \) is the \( ij^{th} \) entry of \( A \in \mathcal{I} \) and \( b \) is the \( kl^{th} \) entry of \( B \in \mathcal{I} \). Let \( M_{ij} \) be a matrix with 1 in the \( ij^{th} \) position and 0 elsewhere. Then \( M_{11}AM_{11} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I} \)

and

\[
M_{1k}BM_{11} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}.
\]

Therefore, \( \begin{pmatrix} a - b & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I} \), so \( a-b \in J \), whence, \( J \) is a subgroup. Fix \( r \in R \). Then \( \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ra & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I} \), so \( ra \in J \), and \( J \) is an ideal.

c. By the following lemma, and parts a. and b., the ideals of \( \mathbb{Z}/12\mathbb{Z} \times M_2(\mathbb{R}) \) are all sets of the form \( I \times J \), where \( I \in \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{6\}\} \) and \( J \in \{M_2(0), M_2(\mathbb{R})\} \).

**Lemma 2.3** Let \( R \) and \( R' \) rings. Then the ideals of \( R \times R' \) have the form \( I \times J \), where \( I \) is an ideal of \( R \) and \( J \) is an ideal of \( R' \).
Proof: Let $A \subseteq R \times R'$ be an ideal. I will show (i) $A = A_1 \times A_2$, for some $A_1 \subseteq R$ and $A_2 \subseteq R'$, and (ii) $A_1$ and $A_2$ are ideals of $R$ and $R'$, respectively.

(i) Define

$$A_1 = \{a \in R : (a, a') \in A \text{ for some } a' \in R'\} \quad \text{and} \quad A_2 = \{a' \in R' : (a, a') \in A \text{ for some } a \in R\}.$$ 

That is, $A_1$ (resp. $A_2$) is the set of all first (resp. second) coordinates of elements in $A$. I claim that $A = A_1 \times A_2$.\footnote{Although this may seem trivial, and to some extent it is trivial, there is something to verify here, since we could have $(a, a') \in A$, $(b, b') \in A$, so that $(a, b') \in A_1 \times A_2$, and yet $(a, b') \notin A$. That is, in general, $A$ need not be equal to the product of all first and second coordinates of elements of $A$. (Consider, for example, the diagonal $\{(0, 0), (1, 1), (2, 2)\}$, which cannot be written as $A_1 \times A_2$.)}

Fix $a \in A_1$ and $b' \in A_2$. We show $(a, b') \in A$. Since $a \in A_1$, there is some $a' \in A_2$ such that $(a, a') \in A$. Similarly, $(b, b') \in A$, for some $b \in A_1$. Since $A$ is an ideal, $(1, 0) \cdot (a, a') = (a, 0) \in A$, and $(0, 1) \cdot (b, b') = (0, b') \in A$. Therefore, $(a, 0) + (0, b') = (a, b') \in A$, as claimed. This proves $A_1 \times A_2 \subseteq A$. The reverse inclusion is obvious.

(ii) Fix $a, b \in A_1$. Then, there exist $a', b' \in A_2$ such that $(a, a') \in A$ and $(b, b') \in A$. Now, since $A$ is, in particular, a subgroup of the additive group of $R \times R'$, we have $(a, a') - (b, b') = (a - b, a' - b') \in A$. Therefore, $a - b \in A_1$, so $A_1$ is a subgroup of $(R, +, 0)$. Fix $r \in R$. Then $(ra, a') = (ra, 1a') = (r, 1) \cdot (a, a') \in A$, since $A$ is an ideal of $R \times R'$. Therefore, $ra \in A_1$, which proves that $A_1$ is an ideal of $R$. The same argument, mutatis mutandis, proves that $A_2$ is an ideal of $R'$. This completes the proof of (ii) and establishes the lemma. \hfill $\square$

3. Let $R$ be a commutative ring and let $A, B$, and $C$ be $R$-modules with $A$ a submodule of $B$. Which (if any) of the following conditions guarantee that the natural map $A \otimes_R C \to B \otimes_R C$ is injective?

(a) $C$ is free,
(b) $C$ is projective.

Solution: I will prove a slightly more general result (as the increased generality comes at no additional cost).

That is, if $\varphi : A \to B$ is an $R$-module monomorphism, then, under conditions (a) or (b), the natural map $\varphi \otimes 1_C : A \otimes_R C \to B \otimes_R C$ is injective. (To answer the question above, take $\varphi$ to be the inclusion map.)

We begin with the simplest case, where $C = R$.

Claim 1: If $\varphi : A \to B$ is an $R$-module monomorphism, then the natural map $\varphi \otimes 1_R : A \otimes_R R \to B \otimes_R R$ is injective.

Proof 1: Define $\alpha_A : A \otimes_R R \cong A$ by $\alpha_A(a \otimes r) = ar$, and $\alpha_B : B \otimes_R R \cong B$ by $\alpha_B(b \otimes r) = br$. (See lemma 2.5 below for proof that these are, indeed, isomorphisms.) I claim that the following diagram of $R$-module homomorphisms is commutative:

$$
\begin{array}{ccc}
A \otimes_R R & \xrightarrow{\alpha_A} & A \\
\varphi \otimes 1_R & & \downarrow{\varphi} \\
B \otimes_R R & \xrightarrow{\alpha_B} & B
\end{array}
$$

Fix $a \in A$ and $r \in R$. By definition, $(\varphi \otimes 1_R)(a \otimes r) = \varphi(a) \otimes 1_R(r)$. Therefore, $(\alpha_B(\varphi \otimes 1_R))(a \otimes r) = \alpha_B(\varphi(a) \otimes r) = \varphi(a)r$. Following the diagram in the other direction, $\varphi(\alpha_A(a \otimes r)) = \varphi(ar) = \varphi(a)r$, since $\varphi$ is an $R$-module homomorphism. Therefore, $(\alpha_B(\varphi \otimes 1_R))(a \otimes r) = (\varphi \alpha_A)(a \otimes r)$. Since $a \in A$ and $r \in R$ were chosen arbitrarily, $\alpha_B(\varphi \otimes 1_R)$ and $\varphi \alpha_A$ agree on generators, so the diagram is commutative.

Now $\alpha_A$ is an isomorphism, so $\alpha_A$ and $\varphi$ are both injective. Therefore, by lemma 2.7 (below), $\varphi \alpha_A$ is injective. Then, by commutativity of the diagram, $\alpha_B(\varphi \otimes 1_R)$ is injective. Finally, lemma 2.9 implies that $\varphi \otimes 1_R$ is injective, which proves claim 1.
Next, let $C$ be a free $R$-module. Then $C \cong \sum_{i \in I} R$, for some index set $I$. For ease of notation, in the sequel, $\sum$ denotes $\sum_{i \in I} R$.

**Claim 2:** If $\varphi : A \rightarrow B$ is an $R$-module monomorphism, then the natural map $\varphi \otimes 1_{\sum R} : A \otimes R \sum R \rightarrow B \otimes R \sum R$ is injective.

**Proof 2:** Define $\Phi : \sum A \rightarrow \sum B$ by $\Phi(\{a_i\}) = \{\varphi(a_i)\}$ for each $\{a_i\} \in \sum A$. Then $\Phi$ is an $R$-module monomorphism. This is seen as follows: $(\forall \{a_i\}, \{a'_i\} \in \sum A) \ (\forall r \in R)$

$$\Phi(\{a_i\} + \{a'_i\}) = \{\varphi(a_i) + \varphi(a'_i)\} = \{\varphi(a_i)\} + \{\varphi(a'_i)\} = \Phi(\{a_i\}) + \Phi(\{a'_i\}),$$

and

$$\Phi(r\{a_i\}) = \{r\varphi(a_i)\} = r\{\varphi(a_i)\} = r\Phi(\{a_i\}).$$

If $\Phi(\{a_i\}) = \{0\} \in \sum B$, then $\{\varphi(a_i)\} = 0$, which implies $\varphi(a_i) = 0$ for all $i \in I$, and therefore, $\{a_i\} = 0 \in \sum A$. Thus, $\Phi$ is a monomorphism.

By (the proof of) lemma 2.5, the map $\sigma : \sum A \rightarrow \sum (A \otimes_R R)$ given by $\sigma(\{a_i\}) = \{a_i \otimes 1_{\sum R}\}$ is an isomorphism.

By (the proof of) lemma 2.6, there is an isomorphism $\tau : \sum (A \otimes_R R) \rightarrow A \otimes_R \sum R$, defined on generators by

$$\tau(a \otimes r, 0, \ldots) = a \otimes (r, 0, \ldots), \quad \tau(0, a \otimes r, 0, \ldots) = a \otimes (0, r, 0, \ldots), \ldots,$$

and

$$\tau(a_1 \otimes r_1, a_2 \otimes r_2, \ldots) = \tau((a_1 \otimes r_1, 0, \ldots) + (0, a_2 \otimes r_2, 0, \ldots) + \cdots)$$

$$= \tau(a_1 \otimes r_1, 0, \ldots) + \tau(0, a_2 \otimes r_2, 0, \ldots) + \cdots$$

$$= a_1 \otimes (r_1, 0, \ldots) + a_2 \otimes (0, r_2, 0, \ldots) + \cdots.$$

(The sum has finitely many non-zero terms, since $\{a_i\}$ is non-zero for finitely many indices $i \in I$.)

Consider the following diagram of $R$-module homomorphisms:

$$\sum A \quad \quad \sum (A \otimes_R R) \quad \quad A \otimes_R \sum R$$

$$\Phi \quad \quad \tau \downarrow \quad \quad \varphi \otimes 1_{\sum R}$$

$$\sum B \quad \quad \sum (B \otimes_R R) \quad \quad B \otimes_R \sum R$$

where $\bar{\sigma}$ and $\bar{\tau}$ are the same maps as their bar-less counterparts, but defined on $\sum B$ and $\sum (B \otimes_R R)$, respectively. I claim that diagram (5) is commutative. Indeed, for any $\{a_i\} \in \sum A$, we have$^{26}$

$$\tau \sigma(\{a_i\}) = \tau(\{a_i \otimes 1_{\sum R}\}) = \tau((a_1 \otimes 1_{\sum R}, 0, \ldots) + (0, a_2 \otimes 1_{\sum R}, 0, \ldots) + \cdots)$$

$$= a_1 \otimes (1_{\sum R}, 0, 1_{\sum R}, 0, \ldots) + a_2 \otimes (0, 1_{\sum R}, 0, \ldots) + \cdots$$

$$\therefore (\varphi \otimes 1_{\sum R}) \tau \sigma(\{a_i\}) = (\varphi \otimes 1_{\sum R})(a_1 \otimes (1_{\sum R}, 0, 1_{\sum R}, 0, \ldots) + a_2 \otimes (0, 1_{\sum R}, 0, \ldots) + \cdots)$$

$$= (\varphi \otimes 1_{\sum R})(a_1 \otimes 1_{\sum R}) + (\varphi \otimes 1_{\sum R})(a_2 \otimes 0, 1_{\sum R}, 0, \ldots) + \cdots$$

$$= \varphi(a_1) \otimes 1_{\sum R} + \varphi(a_2) \otimes 0, 1_{\sum R}, 0, \ldots + \cdots.$$

In the other direction, $\bar{\sigma} \Phi(\{a_i\}) = \bar{\sigma}(\{\varphi(a_i)\}) = \{\varphi(a_i) \otimes 1_{\sum R}\}$, so

$$\bar{\tau} \bar{\sigma} \Phi(\{a_i\}) = \bar{\tau}(\{\varphi(a_i) \otimes 1_{\sum R}\}) = \tau((\varphi(a_1) \otimes 1_{\sum R}, 0, \ldots) + (\varphi(a_2) \otimes 1_{\sum R}, 0, \ldots) + \cdots)$$

$$= \varphi(a_1) \otimes 1_{\sum R} + \varphi(a_2) \otimes 0, 1_{\sum R}, 0, \ldots + \cdots.$$

$^{26}$Again, the sums have finitely many non-zero terms, since $\{a_i\}$ is non-zero for finitely many indices $i \in I$. The same comment applies to the sums in the following two sets of equations.
which proves that \( \bar{\tau} \bar{\sigma} \Phi \) and \( (\varphi \otimes 1_{\Sigma R}) \tau \sigma \) agree on generators. Therefore, diagram (5) is commutative.

Now, \( \sigma \) and \( \bar{\tau} \) are \( R \)-module isomorphisms, and \( \Phi \) is an \( R \)-module monomorphism. Therefore, by lemma 2.7 below, \( \bar{\tau} \bar{\sigma} \Phi \) is an \( R \)-module monomorphism, so commutativity of (5) implies that \( \varphi \otimes 1_{\Sigma R} \tau \sigma \) is also an \( R \)-module monomorphism. Finally, since \( \sigma \) and \( \bar{\tau} \) are isomorphisms, so is \( \tau \sigma \). Whence, \( \varphi \otimes 1_{\Sigma R} \) is injective, by lemma 2.8. This which proves claim 2 and completes part (a) of the problem.

**Claim 3:** If \( C \) is a projective \( R \)-module and \( \varphi : A \to B \) is an \( R \)-module monomorphism, then the natural map \( \varphi \otimes 1_C : A \otimes R C \to B \otimes R C \) is injective.

**Proof 3:** Since \( C \) is projective, there exists a free \( R \)-module \( F \) and a (projective) \( R \)-module \( D \) such that \( F = C \oplus D \) (lemma 2.4). Therefore,

\[
A \otimes_R F = A \otimes_R (C \oplus D) \cong (A \otimes_R C) \oplus (A \otimes_R D) \quad \text{and} \quad B \otimes_R F = B \otimes_R (C \oplus D) \cong (B \otimes_R C) \oplus (B \otimes_R D),
\]

where the isomorphisms are given by lemma 2.6.

By claim 2 above, the natural map \( \varphi \otimes 1_F : A \otimes_R F \to B \otimes_R F \) is injective. Consider the diagram

\[
\begin{array}{ccc}
A \otimes_R C & \xrightarrow{\varphi \otimes 1_C} & (A \otimes_R C) \oplus (A \otimes_R D) \\
\uparrow \varphi \otimes 1_C & & \Downarrow \varphi \otimes 1_F \\
B \otimes_R C & \xrightarrow{\bar{\tau} \otimes 1_C} & (B \otimes_R C) \oplus (B \otimes_R D)
\end{array}
\]

By (the proof of) lemma 2.6 the map \( \tau : (A \otimes_R C) \oplus (A \otimes_R D) \to A \otimes_R (C \oplus D) \) given by \( \tau(a_1 \otimes c, a_2 \otimes d) = a_1 \otimes (c, 0) + a_2 \otimes (0, d) \) is an \( R \)-module isomorphism. Given \( a \otimes c \in A \otimes_R C \), then,

\[
(\varphi \otimes 1_F) \tau \iota_1 (a \otimes c) = (\varphi \otimes 1_F) \tau(a \otimes c, 0) = (\varphi \otimes 1_F)(a \otimes (c, 0)) = \varphi(a) \otimes (c, 0).
\]

Similarly, there exists \( \bar{\tau} : (B \otimes_R C) \oplus (B \otimes_R D) \cong B \otimes_R (C \oplus D), \) with \( \bar{\tau}(b_1 \otimes c, b_2 \otimes d) = b_1 \otimes (c, 0) + b_2 \otimes (0, d), \) and \( \bar{\tau} \iota_1 (\varphi \otimes 1_C)(a \otimes c) = \bar{\tau}(\varphi(a) \otimes c, 0) = \varphi(a) \otimes (c, 0). \)

Therefore, \( (\varphi \otimes 1_F) \tau \iota_1 \) and \( \bar{\tau} \iota_1 (\varphi \otimes 1_C) \) agree on generators of \( A \otimes_R C \), so diagram (6) is commutative.

By lemma 2.7, \( (\varphi \otimes 1_F) \tau \iota_1 \) is injective, so, by commutativity, \( \bar{\tau} \iota_1 (\varphi \otimes 1_C) \) is injective. It now follows from lemma 2.9 that \( \varphi \otimes 1_C \) is injective, which completes the proof of claim 3 and part (b) of the problem.

The following six lemmas are used in the answer to problem 3 given above. The first is a standard theorem about projective modules, the proof of which is not hard, and can be found, e.g., in Hungerford. The next two lemmas (2.5 and 2.6) are also standard, but I haven’t seen them proved in detail elsewhere and, as the solution given above makes repeated use of the maps defined in proving these lemmas, I include detailed proofs below. The last three lemmas are trivial verifications.

**Lemma 2.4** Let \( R \) be a ring. The following conditions on an \( R \)-module \( P \) are equivalent:

(i) \( P \) is projective;

(ii) every short exact sequence of \( R \)-modules \( 0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0 \) is split exact (hence \( B \cong A \oplus P \));

(iii) there is a free \( R \)-module \( F \) and an \( R \)-module \( N \) such that \( F \cong N \oplus P \).

**Lemma 2.5** If \( R \) is a commutative ring with \( 1_R \) and \( A \) is a unitary \( R \)-module, then \( A \otimes_R R \cong A \).
Proof: Define $\alpha : A \times R \to A$ by $\alpha(a,r) = ar$. Since $\alpha$ is clearly bilinear, there exists a unique $R$-module homomorphism $\bar{\alpha} : A \otimes_R R \to A$ such that $\bar{\alpha} = \alpha$, where $\bar{\alpha} : A \times R \to A \otimes_R R$ is the canonical bilinear map. Define $\beta : A \to A \otimes_R R$ by $\beta(a) = a \otimes 1_R$. Then it is easy to verify that $\beta$ is an $R$-module homomorphism and that

$$\beta \bar{\alpha}(a \otimes r) = \beta(ar) = ar \otimes 1_R = a \otimes r \quad (\forall a \in A)(\forall r \in R).$$

Therefore, $\beta \bar{\alpha}$ is the identity on generators of $A \otimes_R R$. Also, $\bar{\alpha}(a) = \bar{\alpha}(a \otimes 1_R) = a1_R = a$, so $\bar{\alpha} = 1_A$. Therefore, $\bar{\alpha} : A \otimes_R R \cong A$.

Lemma 2.6 Let $R$ be a commutative ring with $1_R$ and let $A, B, C$ be unitary $R$-modules. Then $A \otimes_R (B \oplus C) \cong (A \otimes_R B) \oplus (A \otimes_R C)$.

Proof: Recall that if $\varphi_1 : A_1 \to D$ and $\varphi_2 : A_2 \to D$ are (group) homomorphisms, then there is a unique homomorphism $\Phi : A_1 \oplus A_2 \to D$ such that $\Phi i_1 = \varphi_1$ and $\Phi i_2 = \varphi_2$, where $i_1 : A_1 \to A_1 \oplus A_2$ and $i_2 : A_2 \to A_1 \oplus A_2$ are the canonical injections. In other words, $\exists! \Phi \in \text{Hom}(A_1 \oplus A_2, D)$ such that the following diagram is commutative:

$$
\begin{array}{ccc}
A_1 & \xrightarrow{i_1} & A_1 \oplus A_2 & \xleftarrow{i_2} & A_2 \\
\downarrow{\varphi_1} & & \downarrow{\Phi} & & \downarrow{\varphi_2} \\
D & & & & D
\end{array}
$$

We can apply this theorem to the Abelian group $(A \otimes_R B) \oplus (A \otimes_R C)$. Let $\varphi_1 : A \times B \to A \otimes_R (B \oplus C)$ be given by $\varphi_1(a,b) = a \otimes (b, 0)$, and let $\varphi_2 : A \times C \to A \otimes_R (B \oplus C)$ be given by $\varphi_2(a,c) = a \otimes (0, c)$. It is easily verified that $\varphi_1$ are bilinear and thus induce $R$-module homomorphisms $\bar{\varphi}_1 : A \otimes_R B \to A \otimes_R (B \oplus C)$ and $\bar{\varphi}_2 : A \otimes_R C \to A \otimes_R (B \oplus C)$ such that $\bar{\varphi}_i \kappa_i = \varphi_1$, where $\kappa_1 : A \times B \to A \otimes_R B$ and $\kappa_2 : A \times C \to A \otimes_R C$ are the canonical bilinear maps. Therefore, the two universal properties combine to give a unique homomorphism $\Phi : (A \otimes_R B) \oplus (A \otimes_R C) \to A \otimes_R (B \oplus C)$ such that the following diagram is commutative:

$$
\begin{array}{ccc}
A \otimes_R B & \xrightarrow{i_1} & (A \otimes_R B) \oplus (A \otimes_R C) & \xleftarrow{i_2} & A \otimes_R C \\
\downarrow{\kappa_1} & & \downarrow{\Phi} & & \downarrow{\kappa_2} \\
A \times B & \xrightarrow{\varphi_1} & A \otimes_R (B \oplus C) & \xrightarrow{\phi} & A \times B
\end{array}
$$

Now, for all $a \in A$ and $b \in B$, $\kappa_1(a \otimes b) = (a \otimes (b, 0))$ and $\bar{\varphi}_1(a \otimes b) = \bar{\varphi}_1 \kappa_1(a,b) = \varphi_1(a,b) = a \otimes (b, 0)$, so, $\Phi(a \otimes b, 0) = a \otimes (b, 0)$. Similarly, $\Phi(0, a \otimes c) = a \otimes (0, c)$, for all $a \in A$ and $c \in C$. Therefore,

$$\Phi(a \otimes b, a' \otimes c) = \Phi(a \otimes b, 0) + \Phi(0, a' \otimes c) = a \otimes (b, 0) + a' \otimes (0, c) \quad (\forall a, a' \in A, b \in B, c \in C).$$

Next, define $\psi : A \times (B \oplus C) \to (A \otimes_R B) \oplus (A \otimes_R C)$ by $\psi(a, (b, c)) = (a \otimes b, a \otimes c)$. Again, $\psi$ is bilinear, so there is a unique $\Psi : A \otimes_R (B \oplus C) \to (A \otimes_R B) \oplus (A \otimes_R C)$ such that $\Psi \kappa = \psi$ where $\kappa : A \times (B \oplus C) \to A \otimes_R (B \oplus C)$ is canonical. To complete the proof, we check that $\Psi \Phi$ and $\Phi \Psi$ given the appropriate identity maps:

$$\Psi \Phi(a \otimes b, 0) = \Psi(a \otimes (b, 0)) = (a \otimes b, a \otimes 0) = (a \otimes b, 0), \text{ and}
$$

$$\Psi \Phi(0, a \otimes c) = \Psi(a \otimes (0, c)) = (a \otimes 0, a \otimes c) = (0, a \otimes c).$$

Thus, $\Psi \Phi$ is the identity on generators of $(A \otimes_R B) \oplus (A \otimes_R C)$, so $\Psi \Phi = 1_{(A \otimes_R B) \oplus (A \otimes_R C)}$. Finally,

$$\Phi \Psi(a \otimes (b, c)) = \Phi(a \otimes b, a \otimes c) = \Phi((a \otimes b, 0) + (0, a \otimes c)) = a \otimes (b, 0) + a \otimes (0, c) = a \otimes (b, c).$$

Thus $\Phi \Psi$ is the identity on generators of $A \otimes_R (B \oplus C)$, so $\Phi \Psi = 1_{A \otimes_R (B \oplus C)}$. This proves that $\Phi : (A \otimes_R B) \oplus (A \otimes_R C) \cong A \otimes_R (B \oplus C)$.
Proof: $fgh(a) = 0 \Rightarrow gh(a) = 0$ (since $f$ is injective) $\Rightarrow h(a) = 0$ (since $g$ is injective) $\Rightarrow a = 0$ (since $h$ is injective). □

Lemma 2.8 If $g \in \text{Hom}_R(A, B)$, $f \in \text{Hom}_R(B, C)$, if $g$ is surjective, and if $fg$ is injective, then $f$ is injective.

Proof: Suppose $f(b) = 0$. Since $g$ is surjective, there is an $a \in A$ such that $g(a) = b$. Then $fg(a) = f(b) = 0$, which implies $a = 0$, since $fg$ is injective. Therefore, $b = g(a) = g(0) = 0$ since $g$ is a homomorphism. □

Lemma 2.9 If $g \in \text{Hom}_R(A, B)$, $f \in \text{Hom}_R(B, C)$, and if $fg$ is injective, then $g$ is injective.

Proof: $\ker g = \{a \in A : g(a) = 0\} \subseteq \{a \in A : fg(a) = 0\} = \ker fg = \{0\}$. The set containment holds since $f$ is a homomorphism, so $f(0) = 0$. □
A BASIC DEFINITIONS AND THEOREMS

APPENDIX

A Basic Definitions and Theorems

A.1 Algebras

An algebra\(^{27}\) (or universal algebra) \(A\) is an ordered pair \(A = (A, F)\) where \(A\) is a nonempty set and \(F\) is a family of finitary operations on \(A\). The set \(A\) is called the universe of \(A\), and the elements \(f^A \in F\) are called the fundamental operations of \(A\). (In practice we prefer to write \(f\) for \(f^A\) when this doesn’t cause ambiguity.\(^{28}\)) The arity of an operation is the number of operands upon which it acts, and we say that \(f \in F\) is an \(n\)-ary operation on \(A\) if \(f\) maps \(A^n\) into \(A\). An operation \(f \in F\) is called a nullary operation (or constant) if its arity is zero. Unary, binary, and ternary operations have arity 1, 2, and 3, respectively. An algebra \(A\) is called unary if all of its operations are unary. An algebra \(A\) is finite if \(|A|\) is finite and trivial if \(|A| = 1\). Given two algebras \(A\) and \(B\), we say that \(B\) is a reduct of \(A\) if both algebras have the same universe and \(A\) can be obtained from \(B\) by simply adding more operations.

Examples

groupoid \(A = (A, \cdot)\)
An algebra with a single binary operation is called a groupoid. This operation is usually denoted by + or \(\cdot\), and we write \(a + b\) or \(a \cdot b\) (or just \(ab\)) for the image of \((a, b)\) under this operation, and call it the sum or product of \(a\) and \(b\), respectively.

semigroup \(A = (A, \cdot)\)
A groupoid for which the binary operation is associative is called a semigroup. That is, a semigroup is a groupoid with binary operation satisfying \((a \cdot b) \cdot c = a \cdot (b \cdot c)\), for all \(a, b, c \in A\).

monoid \(A = (A, \cdot, e)\)
A monoid is a semigroup along with a multiplicative identity \(e\). That is, \((A, \cdot)\) is a semigroup and \(e\) is a constant (nullary operation) satisfying \(e \cdot a = a \cdot e = a\), for all \(a \in A\).

group \(A = (A, \cdot, e)\)
A group is a monoid along with a unary operation \(^{-1}\) called multiplicative inverse. That is, the reduct \((A, \cdot, e)\) is a monoid and \(^{-1}\) satisfies \(a \cdot a^{-1} = a^{-1} \cdot a = e\), for all \(a \in A\). An Abelian group is a group with a commutative binary operation, which we usually denote by + instead of \(\cdot\). In this case, we write 0 instead of \(e\) to denote the additive identity, and \(-\) instead of \(^{-1}\) to denote the additive inverse. Thus, an Abelian group is a group \(A = (A, +, 0)\) such that \(a + b = b + a\) for all \(a, b \in A\).

ring \(A = (A, +, \cdot, 0)\)
A ring is an algebra \(A = (A, +, \cdot, 0)\) such that

R1. \((A, +, 0)\) is an Abelian group,

R2. \((A, \cdot)\) is a semigroup, and

R3. for all \(a, b, c \in A\), \(a \cdot (b + c) = a \cdot b + a \cdot c\) and \((a + b) \cdot c = a \cdot c + b \cdot c\).

A ring with unity (or unital ring) is an algebra \(A = (A, +, \cdot, 0, 1)\), where the reduct \((A, +, \cdot, 0)\) is a ring, and where 1 is a multiplicative identity; i.e. \(a \cdot 1 = 1 \cdot a = a\), for all \(a \in A\).

\(^{27}\)N.B. In this first paragraph, not all of the definitions are entirely precise. Rather, my goal here is to state them in a way that seems intuitive and heuristically useful.

\(^{28}\)This convention creates an ambiguity when discussing, for example, homomorphisms from one algebra, \(A\), to another, \(B\); in such cases we will adhere to the more precise notation \(f^A\) and \(f^B\), for operations on \(A\) and \(B\), respectively.
field If \( A = \langle A, +, \cdot, -, 0, 1 \rangle \) is a ring with unity, an element \( r \in A \) is called a unit if it has a multiplicative inverse. That is, \( r \in A \) is a unit provided there exists \( r^{-1} \in A \) with \( r \cdot r^{-1} = r^{-1} \cdot r = 1 \). A division ring is a ring in which every non-zero element is a unit, and a field is a division ring in which multiplication is commutative.

module Let \( R = \langle R, +, \cdot, -, 0, 1 \rangle \) be a ring with unit. An \( R \)-module (sometimes called a left unitary \( R \)-module) is an algebra \( M = \langle M, +, -, 0, f_r \rangle_{r \in R} \) with an Abelian group reduct \( \langle M, +, -, 0 \rangle \), and with unary operations \( (f_r)_{r \in R} \) which satisfy the following four conditions for all \( r, s \in R \) and \( x, y \in M \):

\[
\begin{align*}
\text{M1. } & f_r(x + y) = f_r(x) + f_r(y) \\
\text{M2. } & f_{r+s}(x) = f_r(x) + f_s(x) \\
\text{M3. } & f_r(f_s(x)) = f_{rs}(x) \\
\text{M4. } & f_1(x) = x.
\end{align*}
\]

If the ring \( R \) happens to be a field, an \( R \)-module is typically called a vector space over \( R \).

Note that condition M1 says that each \( f_r \) is an endomorphism of the Abelian group \( \langle M, +, -, 0 \rangle \). Conditions M2–M4 say: (1) the collection of endomorphisms \( (f_r)_{r \in R} \) is itself a ring with unit, where the function composition described in (M3) is the binary multiplication operation, and (2) the map \( r \mapsto f_r \) is a ring epimorphism from \( R \) onto \( (f_r)_{r \in R} \).

Part of the importance of modules lies in the fact that every ring is, up to isomorphism, a ring of endomorphisms of some Abelian group. This fact is analogous to the more familiar theorem of Cayley stating that every group is isomorphic to a group of permutations of some set.

bilinear algebra Let \( F = \langle F, +, -, 0, 1 \rangle \) be a field. An algebra \( A = \langle A, +, -, 0, f_r \rangle_{r \in F} \) is a bilinear algebra over \( F \) provided \( \langle A, +, -, 0, f_r \rangle_{r \in F} \) is a vector space over \( F \) and for all \( a, b, c \in A \) and all \( r \in F \),

\[
\begin{align*}
(a + b) \cdot c &= (a \cdot c) + (b \cdot c) \\
c \cdot (a + b) &= (c \cdot a) + (c \cdot b) \\
a \cdot f_r(b) &= f_r(a \cdot b) = f_r(a) \cdot b
\end{align*}
\]

If, in addition, \((a \cdot b) \cdot c = a \cdot (b \cdot c)\) for all \( a, b, c \in A \), then \( A \) is called an associative algebra over \( F \). Thus an associative algebra over a field has both a vector space reduct and a ring reduct. An example of an associative algebra is the space of linear transformations (endomorphisms) of any vector space into itself.

A.2 Congruence Relations and Homomorphisms

Let \( A \) be a set. A binary relation \( \theta \) on \( A \) is a subset of \( A^2 = A \times A \). If \( \langle a, b \rangle \in \theta \) we sometimes write \( a \theta b \). The diagonal relation on \( A \) is the set \( \Delta_A = \{ \langle a, a \rangle : a \in A \} \) and the all relation is the set \( \nabla_A = A^2 \). (We write \( \Delta \) and \( \nabla \) when the underlying set is apparent.)

equivalence A binary relation \( \theta \) on a set \( A \) is an equivalence relation on \( A \) if, for any \( a, b, c \in A \), it satisfies:

\[
\begin{align*}
\text{E1. } & \langle a, a \rangle \in \theta, \\
\text{E2. } & \langle a, b \rangle \in \theta \text{ implies } \langle b, a \rangle \in \theta, \text{ and} \\
\text{E3. } & \langle a, b \rangle \in \theta \text{ and } \langle b, c \rangle \in \theta \text{ imply } \langle a, c \rangle \in \theta.
\end{align*}
\]

We denote the set of all equivalence relations on \( A \) by \( \text{Eq}(A) \).

If \( \theta \in \text{Eq}(A) \) is an equivalence relation on \( A \) and \( \langle x, y \rangle \in \theta \), we say that \( x \) and \( y \) are equivalent modulo \( \theta \). The set of all \( y \in A \) that are equivalent to \( x \) modulo \( \theta \) is denoted by \( x/\theta = \{ y \in A : \langle x, y \rangle \in \theta \} \) and we call \( x/\theta \)
the equivalence class (or coset) of $x$ modulo $\theta$. The set $\{x/\theta : x \in A\}$ of all equivalence classes of $A$ modulo $\theta$ is denote by $A/\theta$. Clearly equivalence classes form a partion of $A$, which simply means that $A = \bigcup_{x \in A} x/\theta$ and $x/\theta \cap y/\theta = \emptyset$ if $x/\theta \neq y/\theta$.

To be continued...
A.3 Group Theory Basics

We begin by collecting some facts that are very useful for solving elementary problems in group theory. (Notation: $H \trianglelefteq G$ means ‘$H$ is a subgroup of $G$’.)

1. $\text{Aut}(G)$ denotes the group of automorphisms of the group $G$. The set of inner automorphisms, denoted $\text{Inn}(G)$, is the (normal) subgroup of $\text{Aut}(G)$ defined as follows: $\varphi \in \text{Inn}(G)$ iff $(\exists g \in G) \ (\forall x \in G) \ (\varphi(x) = gxg^{-1})$.

2. Let $H \trianglelefteq G$ and let $A \subseteq \text{Aut}(G)$ be a non-empty set of automorphisms of $G$. We say that $H$ is an $A$-invariant subgroup of $G$ if $h^\alpha \in H$ for all $h \in H$ and $\alpha \in A$. For instance, if $A = \{1\}$ then, trivially, every subgroup of $G$ is $A$-invariant. In two important special cases we use special terms. If $H$ is $\text{Aut}(G)$-invariant, $H$ is said to be characteristic in $G$. If $H$ is $\text{Inn}(G)$-invariant, $H$ is said to be normal in $G$.

The concept of normal subgroup dominates the whole of group theory, and a special notation is used. We write $H \trianglelefteq G$ to mean ‘$H$ is a normal subgroup of $G$’, and $H \ntrianglelefteq G$ to mean ‘$H$ is not a normal subgroup of $G$’.

3. The normalizer of a subset $S \subseteq G$ is the set

\[ N_G(S) = \{g \in G : g^{-1}Sg = S\}. \]

In case $S = \{s\}$ is a singleton, we write $N_G(\{s\}) = N_G(s)$. Also, we occasionally denote $N_G(S)$ by $N(S)$ when the context makes clear which overgroup is intended. It is easy to verify that the normalizer is a subgroup of $G$. In fact, when $S$ is a subgroup of $G$, $N_G(S)$ is the largest subgroup of $G$ in which $S$ is normal. Thus, $S \trianglelefteq N_G(S) \trianglelefteq G$, and $S \trianglelefteq G$ iff $N_G(S) = G$.

4. The centralizer of a subset $S \subseteq G$ is the set

\[ C_G(S) = \{g \in G : g^{-1}sg = s \text{ for all } s \in S\}. \]

Here too, we write $C_G(\{s\}) = C_G(s)$ when $S = \{s\}$ is a singleton, in which case we also have $C_G(s) = N_G(s)$. Thus, it is clear from the definition that

\[ C_G(S) = \bigcap_{s \in S} C_G(s) = \bigcap_{s \in S} N_G(s). \]

Next note that, since $S \trianglelefteq N_G(S)$, the group $N_G(S)$ acts on $S$ by conjugation. The map $\tau : N_G(S) \to \text{Aut}(S)$, defined by $\tau(g)(s) = gs^{-1g^{-1}}$ ($\forall s \in S; \ \forall g \in N_G(S)$) is a group homomorphism with kernel

\[ \ker \tau = \{g \in N_G(S) : g^{-1}sg = s \text{ for all } s \in S\}. \]

But notice that if $g \in G$ satisfies $g^{-1}sg = s$ for all $s \in S$, then certainly $g \in N_G(S)$. Therefore,

\[ \ker \tau = \{g \in N_G(S) : g^{-1}sg = s \text{ for all } s \in S\} = \{g \in G : g^{-1}sg = s \text{ for all } s \in S\} = C_G(S). \]

Since kernels of homomorphisms are normal subgroups, we have proven $C_G(S) \trianglelefteq N_G(S)$.

5. A group $G$ is called simple provided $G$ has exactly two normal subgroups, namely $G$ and $\{e\}$ (the identity in $G$). Clearly if $G$ is simple, then any homomorphism on $G$ is a monomorphism (since the kernel of a homomorphism is a normal subgroup). A group $G$ is called almost simple if $G$ has a normal subgroup $S \trianglelefteq G$ which is nonabelian, simple, and has trivial centralizer $C_G(S) = \{e\}$.
Next we review a number of very useful results, as presented in John Dixon’s wonderful little book [1].

1.T.1. If $H \leq K \leq G$ and if $[G : H]$ is finite, then $[G : K]$ is finite and $[G : H] = [G : K][K : H]$. 

1.T.2. If $A, B \leq G$ and $[G : B]$ is finite, then $A \cap B$ is a subgroup of finite index in $A$. In fact, $[A : A \cap B] \leq [G : B]$, with equality iff $G = AB$.

In particular, if $[G : A]$ is also finite, then $[G : A \cap B] \leq [G : A][G : B]$ with equality iff $G = AB$.

1.T.3. If $S$ is a subset of a group $G$, then the number of conjugates, $x^{-1}Sx$ ($x \in G$), of $S$ in $G$ is equal to $[G : N_G(S)]$.

In the case that $S$ consists of a single element $s$, then $N_G(S) = C_G(s)$, and $s$ has $[G : C(s; G)]$ conjugates in $G$.

---

As Dixon notes, the proofs of 1.T.1–3 can be found in Hall (Sec. 1.5–6, 2.1–3); Kurosh (Ch. 3); Rotman (Ch. 2); Schenkman (Sec. 1.1–3); and Scott (Sec. 1.6–7, 2.2–3, 3.1–3).
A.4 Direct Products

D.1. For an arbitrary (possibly infinite) family of groups \( \{ G_i \mid i \in I \} \), define a binary operation on the Cartesian product (of sets) \( \prod_{i \in I} G_i \) as follows: If \( f, g \in \prod_{i \in I} G_i \) (that is, \( f, g : I \to \bigcup_{i \in I} G_i \) and \( f(i), g(i) \in G_i \) for each \( i \)), then \( fg : I \to \bigcup_{i \in I} G_i \) is the function given by \( i \mapsto f(i)g(i) \). Since each \( G_i \) is a group, \( f(i)g(i) \in G_i \) for every \( i \), whence \( fg \in \prod_{i \in I} G_i \). It is easy to verify that \( \prod_{i \in I} G_i \) together with this binary operation is a group, called the direct product (or complete direct sum) of the family of groups \( \{ G_i \mid i \in I \} \).

D.2. The (external) weak direct product of a family of groups \( \{ G_i \mid i \in I \} \), denoted \( \prod^w G_i \), is the set of all \( f \in \prod_{i \in I} G_i \) such that \( f(i) = e_i \), the identity in \( G_i \), for all but finitely many \( i \in I \). If all \( G_i \) are (additive) abelian, then \( \prod^w G_i \) is usually called the (external) direct sum and is denoted \( \sum_{i \in I} G_i \).

If \( I \) is finite, the weak direct product coincides with the direct product.

D.3. Theorem. If \( \{ G_i \mid i \in I \} \) is a family of groups, then \( \prod^w G_i \) is a normal subgroup of \( \prod_{i \in I} G_i \) and, for each \( k \in I \),

\[ (i) \text{ the map } \pi_k : \prod_{i \in I} G_i \to G_k \text{ given by } \pi_k(f) = f(k) \text{ is an epimorphism of groups;} \]

\[ (ii) \text{ the map } \iota_k : G_k \to \prod^w G_i \text{ given by } \iota_k(a) = (e_1, \ldots, e_{k-1}, a, e_k, \ldots) \text{ is a monomorphism of groups;} \]

\[ (iii) \iota_k(G_k) \text{ is a normal subgroup of } \prod_{i \in I} G_i. \]

As a memory aid, the following diagram might help:

\[ 0 \longrightarrow G_k \xrightarrow{\iota_k} \prod^w G_i \xrightarrow{\subseteq} \prod_{i \in I} G_i \xrightarrow{\pi_k} G_k \longrightarrow 0 \]

D.4. Theorem. Let \( \{ N_i \mid i \in I \} \) be a family of normal subgroups of a group \( G \) such that

\[ (i) \ G = \langle \bigcup_{i \in I} N_i \rangle. \]

\[ (ii) \text{ For each } k \in I, N_k \cap \bigcup_{i \neq k} N_i = \langle e \rangle. \]

Then \( G = \prod^w_{i \in I} N_i \).

D.5. The following special case arises frequently: if \( N_i \varsubsetneq G \) for each \( 1 \leq i \leq r \), then \( \langle N_1 \cup N_2 \cup \cdots \cup N_r \rangle = N_1N_2 \cdots N_r = \{ n_1n_2 \cdots n_r \mid n_i \in N_i \} \). In additive notation \( N_1N_2 \cdots N_r \) is written \( N_1 + N_2 + \cdots + N_r \).

D.6. Corollary. If \( N_i \not\subset G \) for each \( 1 \leq i \leq r \), if \( G = N_1N_2 \cdots N_r \), and if \( N_k \cap \langle N_1 \cdots N_{k-1}N_{k+1} \cdots N_r \rangle = \langle e \rangle \) for each \( 1 \leq k \leq r \), then \( G \cong N_1 \times N_2 \times \cdots \times N_r \).
A.5 Ring Theory Basics

**multiplicative** A subset $A$ of a ring (or groupoid) is called *multiplicative* iff it is closed under multiplication; i.e. $x, y \in A$ implies $xy \in A$.

**prime ideal** An ideal $P$ in a ring $R$ is *prime* iff $P \neq R$ and, for any ideals $A, B$ of $R$,

$$AB \subseteq P \implies A \subseteq P \text{ or } B \subseteq P.$$  \hspace{1cm} (7)

**Theorem A.1** If $R$ is a commutative ring, then a proper ideal $P \subsetneq R$ is prime if and only if, for all elements $a, b \in R$,

$$ab \in P \implies a \in P \text{ or } b \in P.$$  \hspace{1cm} (8)

If $R$ is a general (non-commutative) ring, then condition (8) implies $P$ is prime but not conversely.

**Proof:** See Hungerford [2], Theorem III.2.15.

Consider the forward implication of Theorem A.1— i.e. $P$ prime implies condition (8). To see that this does not hold in general for non-commutative rings, consider this simple counter-example: Let $M_2(\mathbb{Z}_2)$ be the ring of $2 \times 2$ matrices over $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ (or over any division ring, for that matter). Then the ideal $P = \{(0)\}$, that is, the ideal generated by the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, is the only ideal of $M_2(\mathbb{Z}_2)$ (this easily follows from Proposition A.1 below.) As the only ideal, $P$ trivially satisfies condition (7), so $P$ is prime. However, if $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, then $ab \in P$, but $a \notin P$ and $b \notin P$.

**Corollary A.1** If $P$ is a prime ideal of a commutative ring $R$, then

$$a_1a_2\cdots a_n \in P \implies a_i \in P \text{ for some } i \in \{1, \ldots, n\}.$$  \hspace{1cm} (9)

Theorem A.1 can also be stated this way:

**Corollary A.2** In a commutative ring $R$, an ideal $P \subsetneq R$ is prime if and only if the set $R \setminus P$ is multiplicative.

**Theorem A.2** If $S$ is a multiplicative subset of a ring $R$ which is disjoint from an ideal $I$ of $R$, then there exists an ideal $P$ which is maximal in the set of all ideals $R$ disjoint from $S$ and containing $I$. Furthermore, any such ideal $P$ is prime.

Note: this theorem is frequently used in the case $I = \{0\}$. (See, e.g., the April 2008 exam 2.10, Problem 2, part d.) To prove the theorem, let $\mathcal{I}$ be the set of all ideals of $R$ which are disjoint from the multiplicative subset $S$. Of course, $\mathcal{I}$ is not empty since $I \in \mathcal{I}$. If $\{I_\lambda : \lambda \in \Lambda\}$ is a chain of ideals in $\mathcal{I}$, it is not hard to show that $J = \bigcup \{I_\lambda : \lambda \in \Lambda\}$ is an ideal, and that $J$ must be disjoint from $S$. Therefore $J \in \mathcal{I}$ and Zorn’s lemma implies that $\mathcal{I}$ contains a maximal ideal. The proof is completed by the following result, which is a useful general principal, so we state it separately as

**Lemma A.1** Suppose $R$ is a commutative ring, $S \subseteq R$ is a multiplicative subset, and $P$ is an ideal of $R$ which is maximal with respect to the property $P \cap S = \emptyset$. Then $P$ is a prime ideal.

**Proof:** Suppose $a, b \in R \setminus P$. We show that $ab \notin P$, which will prove that $P$ is prime. Since $P$ is maximal among all ideals with the property $P \cap S = \emptyset$, we have

$$(P + Ra) \cap S \neq \emptyset \neq (P + Rb).$$

Therefore, $p + ra = s$ for some $p \in P, r \in R$, and $s \in S$, and $p' + r'b = s'$ for some $p' \in P, r' \in R$, and $s' \in S$. Now compute

$$ss' = (p + ra)(p' + r'b) = pp' + pr'b + rap' + rr'ab.$$  \hspace{1cm} (10)

The first three terms on the right are in $P$ since $P$ is an ideal, while the left-hand-side $ss' \in S$, as $S$ is multiplicative. Therefore, $rr'ab$ cannot be in $P$, so $ab \notin P$. \hfill \Box
A.6 Factorization in Commutative Rings

We assume throughout this section that $R$ is a commutative ring with identity $e$. First recall some basic definitions.

**unit** An element of $R$ that has an inverse is called a unit. That is $r \in R$ is a unit iff there is an $a \in R$ with $ar = ra = e$.

**irreducible**

**prime** A nonzero, nonunit element $r$ in a commutative ring $R$ is called

(i) irreducible provided that $r = ab$ implies $a$ or $b$ is a unit

(ii) prime provided that $r|ab$ implies $r|a$ or $r|b$.

A.7 Rings of Polynomials

We review some basic facts about the polynomial rings $R[x]$ and $R[x_1, \ldots, x_n]$. Most of the material in this section has been shamelessly copied from Hungerford ([2], section III.6) – sometimes word-for-word – since, in my opinion, Hungerford’s presentation cannot be improved upon.

Let $R$ be a ring. The **degree of a nonzero monomial** $ax_1^{k_1}x_2^{k_2} \cdots x_n^{k_n} \in R[x_1, \ldots, x_n]$ is the nonnegative integer $k_1 + k_2 + \cdots + k_n$. If $f$ is a nonzero polynomial in $R[x_1, \ldots, x_n]$, then $f = \sum_{i=0}^{m} a_i x_1^{i_1} \cdots x_n^{i_n}$, and the **(total) degree of the polynomial** $f$ is the maximum of the degrees of the monomials $a_i x_1^{i_1} \cdots x_n^{i_n}$ such that $a_i \neq 0$ ($i = 1, 2, \ldots, m$). The total degree of $f$ is denoted $\deg f$. Clearly a nonzero polynomial $f$ has degree zero iff $f$ is a constant polynomial and $f = a_0 = a_0 x_1^0 \cdots x_n^0$. Recall that, for each $1 \leq k \leq n$, $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$ is a subring of $R[x_1, \ldots, x_n]$. The **degree of $f$ in $x_k$** is the degree of $f$ considered as a polynomial in one indeterminate $x_k$ over the ring $R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$.

**Theorem A.3** (i) $\deg(f + g) \leq \max \{ \deg f, \deg g \}$.

(ii) $\deg(fg) \leq \deg f + \deg g$.

(iii) If $R$ has no zero divisors, $\deg(fg) = \deg f + \deg g$.

(iv) If $n = 1$ and the leading coefficient of $f$ or $g$ is not a zero divisor in $R$ (in particular, if it is a unit), then $\deg(fg) = \deg f + \deg g$.

This theorem is also true if $\deg f$ is taken to mean “degree of $f$ in $x_k$.”

It is easy to verify that $R[x]$ is commutative (resp. an integral domain) whenever the same is true of $R$. If $F$ is a field, then $F[x]$ is a Euclidean domain, hence a PID and a UFD, and the set of units of $F[x]$ is precisely the set of nonzero constant polynomials, which can be identified with the set $F^\times = F \setminus \{0\}$. ([2] Theorem 6.14)

If $D$ is a UFD, we have the following important facts about the units and irreducible elements of $D[x]$ ([2], p. 162):

(i) The units in $D[x]$ are precisely the constant polynomials that are units in $D$.

(ii) If $c$ is an irreducible element of $D$, then the constant polynomial $c$ is irreducible in $D[x]$ [use Thm A.3 and (i)].

(iii) Every first degree polynomial whose leading coefficient is a unit in $D$ is irreducible in $D[x]$. In particular, every first degree polynomial over a field is irreducible.

(iv) Suppose $D$ is a subring of an integral domain $E$ and $f \in D[x] \subseteq E[x]$. Then $f$ may be irreducible in $E[x]$ but not in $D[x]$ and vice versa, as is seen in the following examples.
Examples. $2x + 2$ is irreducible in $\mathbb{Q}[x]$ by (iii) above. However, $2x + 2 = 2(x + 1)$ and neither $2$ nor $x + 1$ is a unit in $\mathbb{Z}[x]$ by (i), whence $2x + 2$ is reducible in $\mathbb{Z}[x]$. On the other hand $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but factors in $\mathbb{C}[x]$ as $(x + i)(x - i)$. By (i), neither $x + i$ nor $x - i$ is a unit in $\mathbb{C}[x]$, so $x^2 + 1$ is reducible in $\mathbb{C}[x]$.

If $D$ is a UFD, then so is $D[x_1, \ldots, x_n]$. ([2] Theorem 6.14) Since a field $F$ is trivially a UFD, $F[x_1, \ldots, x_n]$ is a UFD.

A.8 Nakayama’s Lemma

**Theorem A.4** (Nakayama) If $J$ is an ideal in a commutative ring $R$ with identity, $1_R$, then the following conditions are equivalent.

(i) $J$ is contained in every maximal ideal of $R$.

(ii) $1_R - j$ is a unit for every $j \in J$.

(iii) If $A$ is a finitely generated $R$-module such that $JA = A$, then $A = 0$.

(iv) If $B$ is a submodule of a finitely generated $R$-module $A$ such that $JA + B = A$, then $B = A$.

**Remark.** As we will see in the next section, the lemma is true even when $R$ is noncommutative, provided that (i) is replaced with the condition that $J$ is contained in the Jacobson radical of $R$.

**Proof:** (i) $\Rightarrow$ (ii) Suppose (i) holds and suppose $1_R - j$ is not a unit. Then $(1_R - j)$ is a proper ideal, so $(1_R - j) \subseteq M$ for some maximal ideal $M \subseteq R$. Thus, $1_R - j \in M$ and $M \subseteq M$, and we have $j \in M$ so $1_R - j + j = 1_R \in M$. Of course, this implies the contradiction $M = R$. Therefore, $1_R - j$ must be a unit. (ii) $\Rightarrow$ (iii) Suppose (ii) holds and let $A$ be a finitely generated $R$-module with $JA = A$. There is a minimal generating set for $A$, say, $\{a_1, \ldots, a_n\}$. If $A \neq 0$, then $a_1$ is not zero. Recall,

$$JA = \{\sum_{i=1}^{m} j_i x_i \mid j_i \in J, x_i \in A, m \in \mathbb{N}\},$$

where each $x_i \in A$ is of the form $x_i = r_1^1 a_1 + \cdots + r_n^m a_n$, and upon rearranging terms, we see that $j_i x_i = \text{each}$.

A.9 Miscellaneous Results and Examples

Here is a basic fact that is sometimes useful (e.g., in the counter-example after Theorem A.1 above). It is elementary and probably appears as an exercise in some of the standard references, though I have not seen it elsewhere.\(^{30}\)

**Proposition A.1** Let $R$ be a commutative ring with $1_R \neq 0$. Then the ideals of $M_n(R)$ are precisely the subsets $M_n(J) \subseteq M_n(R)$, where $J$ is an ideal of $R$.

**Proof:** We prove it for the case $n = 2$. The proof in the general case should be almost identical. Suppose $J$ is an ideal and $A_1, A_2 \in M_2(J)$. Then $A_1 - A_2$ has all elements in $J$, since $J$ is, in particular, a subgroup. Therefore $M_2(J)$ is a subgroup of $\langle M_2(R); +, 0 \rangle$. If $M = (m_{ij}) \in M_2(R)$ and $A = (a_{ij}) \in M_2(J)$, then $MA = (\sum_{k=1}^{2} m_{ik} a_{kj})$. Clearly, all the elements of $MA$ are in $J$, since $J$ is an ideal and $a_{ij} \in J$. Similarly, all the elements of $AM$ are in $J$. This proves that $M_2(J)$ is an ideal of $M_2(R)$ whenever $J$ is an ideal of $R$.

Now, let $\mathcal{I} \subseteq M_2(R)$ be an ideal of $M_2(R)$, and let $J$ be the set of all $a \in R$ such that $a$ is an element of some $A \in \mathcal{I}$. Clearly $0 \in J$, since $A \in \mathcal{I}$ implies $0 = A - A \in \mathcal{I}$. Let $a, b \in J$. Suppose $a$ is the $ij^{th}$ entry of $A \in \mathcal{I}$ and $b$ is the $kl^{th}$ entry of $B \in \mathcal{I}$. Let $M_{ij}$ be a matrix with $1$ in the $ij^{th}$ position and $0$ elsewhere. Then $M_{ij}AM_{ij} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}$ and $M_{kl}BM_{kl} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}$. Therefore, $\begin{pmatrix} a - b & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}$, so $a - b \in J$, whence, $J$ is a subgroup. Fix $r \in R$. Then $\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ra & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}$, so $ra \in J$, and $J$ is an ideal.

\(^{30}\)I have since found a nice, short proof of this result in Lam’s book [5].
Proposition A.2  Let $R$ and $R'$ rings. Then the ideals of $R \times R'$ have the form $I \times J$, where $I$ is an ideal of $R$ and $J$ is an ideal of $R'$.

Proof: Let $A \subseteq R \times R'$ be an ideal. I will show (i) $A = A_1 \times A_2$, for some $A_1 \subseteq R$ and $A_2 \subseteq R'$, and (ii) $A_1$ and $A_2$ are ideals of $R$ and $R'$, respectively.

(i) Define

$$A_1 = \{a \in R : (a, a') \in A \text{ for some } a' \in R'\} \quad \text{and} \quad A_2 = \{a' \in R' : (a, a') \in A \text{ for some } a \in R\}.$$ 

That is, $A_1$ (resp. $A_2$) is the set of all first (resp. second) coordinates of elements in $A$. I claim that $A = A_1 \times A_2$.\(^{31}\) Fix $a \in A_1$ and $b' \in A_2$. We show $(a, b') \in A$. Since $a \in A_1$, there is some $a' \in A_2$ such that $(a, a') \in A$. Similarly, $(b, b') \in A$, for some $b \in A_1$. Since $A$ is an ideal, $(1, 0) \cdot (a, a') = (a, 0) \in A$, and $(0, 1) \cdot (b, b') = (0, b') \in A$. Therefore, $(a, 0) + (0, b') = (a, b') \in A$, as claimed. This proves $A_1 \times A_2 \subseteq A$. The reverse inclusion is obvious.

(ii) Fix $a, b \in A_1$. Then, there exist $a', b' \in A_2$ such that $(a, a') \in A$ and $(b, b') \in A$. Now, since $A$ is, in particular, a subgroup of the additive group of $R \times R'$, we have $(a, a') - (b, b') = (a - b, a' - b') \in A$. Therefore, $a - b \in A_1$, so $A_1$ is a subgroup of $(R, +, 0)$. Fix $r \in R$. Then $(ra, a') = (ra, 1a') = (r, 1) \cdot (a, a') \in A$, since $A$ is an ideal of $R \times R'$. Therefore, $ra \in A_1$, which proves that $A_1$ is an ideal of $R$. The same argument, mutatis mutandis, proves that $A_2$ is an ideal of $R'$. This completes the proof of (ii) and establishes the proposition. \( \square \)

Example:\(^{32}\) The ideals of $\mathbb{Z}/12\mathbb{Z} \times M_2(\mathbb{R})$ are all sets of the form $I \times J$, where $I \in \{(0), (1), (2), (3), (4), (6)\}$ and $J \in \{M_2(0), M_2(\mathbb{R})\}$.

The following is a nice proof of a standard problem that I learned from the book by Lam [5].

Proposition A.3  Let $R$ be a ring with identity 1. If $a$ and $b$ are nonzero elements in $R$, then $1 - ab$ is invertible if and only if $1 - ba$ is invertible.

Proof: It is clear by symmetry that we need only prove one direction. Suppose $1 - ab$ is invertible. The ideal $R(1 - ba)$ contains $Ra(1 - ba) = R(1 - ab)a = Ra$ and, therefore, contains $1 - ba + ba = 1$. Thus, $R(1 - ba) = R$, which implies $r(1 - ba) = 1$ for some $r \in R$.

A related linear algebra problem is to show that if $A$ and $B$ are square matrices, then $AB$ and $BA$ have the same eigenvalues. This can be solved exactly as above, with one modification: replace 1 with $\lambda I$, where $I$ is the identity matrix of the same dimensions as $A$ and $B$.\(^{32}\)

---

\(^{31}\)Although this may seem trivial, and to some extent it is trivial, there is something to verify here, since we could have $(a, a') \in A$, $(b, b') \in A$, so that $(a, b') \in A_1 \times A_2$, and yet $(a, b') \not\in A$. That is, in general, $A$ need not be equal to the product of all first and second coordinates of elements of $A$. (Consider, for example, the diagonal $\{(0, 0), (1, 1), (2, 2)\}$, which cannot be written as $A_1 \times A_2$.)

\(^{32}\)This example appears in the first problem of the ring theory section of the November 2008 comprehensive exams.
References


