SOLUTION KEY
Produced by: Kyle Dahlin

<u>Problems:</u>
Chap 13: 4, 24, **30**, 31, 32, **42**, 43
Chap 14: 4, 6, **10**, 11, 12, 13, 14

Problem 13.4. List all zero-divisors in $\mathbb{Z}_{20}$. Can you see a relationship between the zero-divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?

Solution:
The zero-divisors of $\mathbb{Z}_{20}$ can be determined by finding all solutions of $ab \equiv 0 \bmod 20$ for integers $1 < a, b < 20$. Hence the zero-divisors are: $\{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$. The set of units of $\mathbb{Z}_{20}$ is the complement of the set of zero-divisors in $\mathbb{Z}_{20}$ without the zero element: $\mathbb{Z}_{20}^{\times} = \{1, 3, 7, 9, 11, 13, 17\}$. ■

Problem 13.24. Find a zero-divisor in $\mathbb{Z}_5[i] = \{a + bi | a, b \in \mathbb{Z}_5\}$.

Solution:
$(2+i)(3+i) = (6-1) + (2+3)i = 0$ in $\mathbb{Z}_5[i]$, so $2+i$ and $3+i$ are zero-divisors in $\mathbb{Z}_5[i]$. ■

Problem 13.30. Let d be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$ is a field.

Solution:
Following **Example 10**, $\mathbb{Q}[\sqrt{d}]$ is a commutative ring. Suppose that there exist $a, b \in \mathbb{Q}$ such that $a^2 - b^2 d = 0$. Then $\sqrt{d} = \frac{a}{b} \in \mathbb{Q}$ and $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}$, which is a field. Otherwise, $a^2 - b^2 d \neq 0$ for all $a, b \in \mathbb{Q}$. Then for any $a, b \in \mathbb{Q}$ with $a, b \neq 0$, $(a + b\sqrt{d})(j + k\sqrt{d}) = 1$, where $j = \frac{a}{a^2 - b^2 d}$ and $k = -\frac{b}{a^2 - b^2 d}$. Hence $\mathbb{Q}[\sqrt{d}]$ is a field. ■

Problem 13.31. Let R be a ring with unity 1. If the product of any pair of nonzero elements of R is nonzero, prove that $ab = 1$ implies $ba = 1$.

Solution:
Suppose that $ab = 1$ and $ba = c$. Then c is nonzero since, by the problem supposition, neither a nor b can be zero. Hence $b = b(ab) = cb$ and so $b(1 - c) = b - cb = 0$. Since $b \neq 0$ and by the supposition, $1 - c = 0$ and thus $ba = c = 1$. ■

Problem 13.32. Let $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field.

Solution:
We start by showing that R is an integral domain. First, R is a commutative ring since it is a subring of the commutative ring $\mathbb{Z}_{10}$. The unity of R is 6. Now if $ab \equiv 0 \bmod 10$, then $5 \mid ab$. But 5 does divide any of the products of pairs of elements of R. Hence R is an integral domain. Since R is also finite, it follows that it is a field by Theorem 13.2. ■

Problem 13.42. Construct a multiplication table for $\mathbb{Z}_2[i]$, the ring of Gaussian integers modulo 2. Is this ring a field? Is it an integral domain?

Solution:

$(\mathbb{Z}_2[i], \times)$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

This is neither a field nor an integral domain, since $(1+i)^2 = 0$. ■

Problem 13.43. The nonzero elements of $\mathbb{Z}_3[i]$ form an Abelian group of order 8 under multiplication. Is it isomorphic to $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

Solution:
Since $1+i$ has multiplicative order 8, the nonzero elements of $\mathbb{Z}_3[i]$ are isomorphic to $\mathbb{Z}_8$ as a group. ■

Problem 14.4. Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Solution:
Let $D = \{(a,a) \mid a \in \mathbb{Z}\}$ be the set of diagonal elements in $\mathbb{Z} \oplus \mathbb{Z}$. This is a subring since $(a,a) - (b,b) = (a-b, a-b) \in D$ and $(a,a) \times (b,b) = (ab, ab) \in D$. However, since $(a,a) \times (1,0) = (a,0) \notin D$, we see that D is not an ideal. ■

Problem 14.6. Find all maximal ideals in

a. $\mathbb{Z}_8$

b. $\mathbb{Z}_{10}$

c. $\mathbb{Z}_{12}$

d. $\mathbb{Z}_n$

Solution:
We follow **Example 14**.

a. $\mathbb{Z}_8$: $\langle 2 \rangle$

b. $\mathbb{Z}_{10}$: $\langle 2 \rangle$ and $\langle 5 \rangle$

c. $\mathbb{Z}_{12}$: $\langle 2 \rangle$ and $\langle 3 \rangle$

d. $\mathbb{Z}_n$: Suppose the prime factorization of n is given by $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. The maximal ideals are $\langle p_1 \rangle$, $\langle p_2 \rangle$, ..., $\langle p_k \rangle$.

■

Problem 14.10. If A and B are ideals of a ring, show that the sum A and B, $A + B = \{a + b | a \in A, b \in B\}$, is an ideal.

Solution:
Let a_1+b_1 and a_2+b_2 be elements of $A+B$. Then $(a_1+b_1)-(a_2+b_2) = (a_1-a_2)+(b_1-b_2) \in A+B$ since A and B are subrings. Now let r be an arbitrary element of the ring. Then ra_1 and a_1r are in A and rb_1 and b_1r are in B since they are ideals. Hence $r(a_1+b_1) = ra_1+rb_1 \in A+B$ and $(a_1+b_1)r = a_1r+b_1r \in A+B$. Thus $A+B$ is an ideal. ∎

Problem 14.11. In the ring of integers, find a positive integer a such that

a. $\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$

b. $\langle a \rangle = \langle 6 \rangle + \langle 8 \rangle$

c. $\langle a \rangle = \langle m \rangle + \langle n \rangle$

Solution:
In general, since $\langle a \rangle \subseteq \langle m \rangle + \langle n \rangle$, $a = ms+nt$ for some $s,t \in \mathbb{Z}$. Next since $\langle a \rangle \supseteq \langle m \rangle + \langle n \rangle$, $m = pa$ and $n = qa$ for some $p,q \in \mathbb{Z}$, meaning a is a common divisor of m and n. Hence a is the greatest common divisor of m and n.

a. Since $\langle a \rangle = \{2s+3t | s,t \in \mathbb{Z}\}$, $a = 1$.

b. Since $\langle a \rangle = \{6s+8t | s,t \in \mathbb{Z}\}$, $a = 2$.

c. Since $\langle a \rangle = \{ms+nt | s,t \in \mathbb{Z}\}$, $a = \gcd(m,n)$.

∎

Problem 14.12. If A and B are ideals of a ring, show that the product of A and B, $AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n | a_i \in A, b_i \in B, n \text{ a positive integer}\}$, is an ideal.

Solution:
Let $c = \sum_{i=1}^n a_ib_i$ and $c' = \sum_{j=1}^m a'_jb'_j$ be arbitrary elements of AB. In particular, each a_ib_i and $a'_jb'_j$ is an element of AB. Then $c - c'$ is clearly in AB, so AB is a subring.

Since A is an ideal, $ra \in A$ for each $a \in A$. And since B is an ideal, $(ra)b \in AB$. Similarly, $abr \in AB$ since $br \in B$. Thus $rc = \sum_{i=1}^n ra_ib_i \in AB$ and $cr \in AB$. ∎

Problem 14.13. Find a positive integer a such that

a. $\langle a \rangle = \langle 3 \rangle \langle 4 \rangle$

b. $\langle a \rangle = \langle 6 \rangle \langle 8 \rangle$

c. $\langle a \rangle = \langle m \rangle \langle n \rangle$

Solution:
By the previous definition of the product of ideals,

$$\langle m \rangle \langle n \rangle = \{r_1ms_1n + r_2ms_2n + \cdots r_kms_kn \mid r_i, s_i \in \mathbb{Z}, k \text{ a positive integer}\}.$$

Since these are integers, this is equivalent to saying $\langle m \rangle \langle n \rangle = \{rmn \mid r \in \mathbb{Z}\} = \langle mn \rangle$. Hence,

a. $\langle 12 \rangle = \langle 3 \rangle \langle 4 \rangle$

b. $\langle 48 \rangle = \langle 6 \rangle \langle 8 \rangle$

c. $\langle mn \rangle = \langle m \rangle \langle n \rangle$

■

Problem 14.14. Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Solution:
Let $c = \sum_{i=1}^{n} a_i b_i \in AB$. Then since A is an ideal, each $a_i b_i \in A$ and hence $c \in A$ since A is a subring. Similarly, $c \in B$. Therefore $c \in A \cap B$ and thus $AB \subseteq A \cap B$. ■