

1. (20 points) Complete 4 of the following 5 definitions.
- A. A commutative ring R with identity is called an *integral domain* if
- B. Let R be a commutative ring. A nonempty subset I of R is called an *ideal* of R if
- C. Let R be a commutative ring with identity 1, and let I be an ideal of R . Then I is called a *principal* ideal of R if
- D. Let R be a commutative ring, and let I be a proper ideal of R . Then I is called a *prime* ideal of R if
- E. A polynomial with integer coefficients is called *primitive* if
2. (20 points) Complete 4 of the following 5 statements of theorems.
- A. (The division algorithm) Let F be a field, and let $f(x)$ and $g(x)$ be polynomials with coefficients in F such that $g(x) \neq 0$. Then
- B. (Eisenstein's irreducibility criterion) Let $f(x) = a_n x^n + \dots + a_0$ be a polynomial with integer coefficients. Then $f(x)$ is irreducible over the field of rational numbers if
- C. Let I be a proper ideal of the commutative ring R with identity 1. Then R/I is an integral domain if and only if
- D. Let I be a proper ideal of the commutative ring R with identity 1. Then R/I is a field if and only if
- E. Let D be an integral domain. Then the characteristic of D is either
3. (30 points) Write out proofs of 2 of the following 3 results from the text.
- A. Any finite integral domain is a field.
- B. In any principal ideal domain every nonzero prime ideal is maximal.
- C. Let F be a field, let $F[x]$ be the ring of polynomials with coefficients in F , and let $p(x)$ be an irreducible polynomial in $F[x]$. Then in the factor ring $F[x]/\langle p(x) \rangle$, every nonzero element is invertible.
4. (15 points) Let R be a commutative ring with identity 1. Let I and J be ideals of R , with $I \subseteq J \subseteq R$. Define $J/I = \{r + I \in R/I \mid r \in J\}$. Define $\phi : R/I \rightarrow R/J$ by $\phi(r + I) = r + J$, for all $r \in R$.
- (a) Show that ϕ is a well-defined ring homomorphism.
- (b) Show that ϕ is onto and that $\ker(\phi) = J/I$.
- (c) Show that $(R/I)/(J/I) \cong R/J$.
5. (15 points) Let F be a field, let $F[x]$ be the ring of polynomials with coefficients in F , let $p(x)$ be a nonzero element of $F[x]$, and let $\langle p(x) \rangle$ be the principal ideal generated by $p(x)$.
- (a) Prove that any element of the factor ring $F[x]/\langle p(x) \rangle$ is either a unit or a zero divisor.
- (b) As an example of part (a), let $F = \mathbf{Z}_2$, and let $p(x) = x^3 + x^2$. In the factor ring $\mathbf{Z}_2[x]/\langle x^3 + x^2 \rangle$, determine which elements are units and which elements are zero divisors.

3. (10 pts) Use Eisenstein's irreducibility criterion to show that $x^4 + 1$ is irreducible over the field \mathbf{Q} .
4. (15 pts) (a) Show that $x^2 + 1$ is irreducible over \mathbf{Z}_3 .
 (b) List the elements of the field $F = \mathbf{Z}_3[x]/\langle x^2 + 1 \rangle$.
 (c) In the multiplicative group of nonzero elements of F , show that $[x + 1]$ is a generator, but $[x]$ is not.
5. (15 pts) Over the field of rational numbers, find the greatest common divisor of $2x^4 - x^3 + x^2 + 3x + 1$ and $2x^3 - 3x^2 + 2x + 2$ and express it as a linear combination of the given polynomials. *Hint:* The answer is linear.
6. (20 pts) Prove the following proposition: Let F be a field, let $F[x]$ be the ring of polynomials with coefficients in F , and let $p(x)$ be a nonzero polynomial in $F[x]$. For any $a(x) \in F[x]$, the congruence class $[a(x)]$ has a multiplicative inverse in $F[x]/\langle p(x) \rangle$ if and only if $\gcd(a(x), p(x)) = 1$.

1. (10 pts) Let I be an ideal of R , and define multiplication of the additive cosets of I by $(r + I)(s + I) = rs + I$ (the standard definition). Prove the result in the text which states that this multiplication is well-defined.
2. (20 pts) Let R be the subset of $\mathbf{Z} \oplus \mathbf{Z}$ defined by $R = \{(m, n) \mid m \equiv n \pmod{2}\}$.
 - (a) Show that R is a subring of $\mathbf{Z} \oplus \mathbf{Z}$.
 - (b) Find all nonzero nilpotent elements of R .
 - (c) Find all nonzero idempotent elements of R .
 - (d) Find all units of R .
3. (20 pts) State and prove the fundamental homomorphism theorem for rings.
4. (30 pts)
 - (a) State the definition of a prime ideal. In the ring \mathbf{Z} , give an example of an ideal that is prime, and an example of an ideal that is not prime. (Explain why or why not.)
 - (b) State the definition of an integral domain. Give an example of an integral domain, and an example of a ring that is *not* an integral domain. (Explain why or why not.)
 - (c) Let I be an ideal of the ring R . Prove the theorem in the text which states that I is a prime ideal of R if and only if R/I is an integral domain.
5. (20 pts) Let R be a subring of S .
 - (a) Show that if I is an ideal of S , then $I \cap R$ is an ideal of R .
 - (b) Prove or disprove: If I is a prime ideal of S then $I \cap R$ is a prime ideal of R .
 - (c) Prove or disprove: If I is a maximal ideal of S then $I \cap R$ is a maximal ideal of R .

EXTRA CREDIT: Let R be a commutative ring with a multiplicative identity 1, and let I and J be proper ideals of R . Show that if there exist $u \in I$ and $v \in J$ with $u + v = 1$, then the direct sum $(R/I) \oplus (R/J)$ is isomorphic to $R/(I \cap J)$. (You may assume that $I \cap J$ is an ideal of R .)

SOLUTIONS

2. (20 pts) Let R be the subset of $\mathbf{Z} \oplus \mathbf{Z}$ defined by $R = \{(m, n) \mid m \equiv n \pmod{2}\}$.
 - (a) Show that R is a subring of $\mathbf{Z} \oplus \mathbf{Z}$.
Use Proposition 5.1.4. If (a, b) and (c, d) belong to R , then $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2}$, so it follows that $a + c \equiv b + d \pmod{2}$ and $ac \equiv bd \pmod{2}$, and thus R is closed under addition and multiplication. Furthermore, $-a \equiv -b \pmod{2}$ implies $-(a, b) \in R$, and it is clear that the identity $(1, 1)$ of $\mathbf{Z} \oplus \mathbf{Z}$ is in R .
 - (b) Find all nonzero nilpotent elements of R .
An element (a, b) in a direct sum is nilpotent if and only if each entry is nilpotent. In an integral domain such as \mathbf{Z} , there are no nonzero nilpotent elements. Since $\mathbf{Z} \oplus \mathbf{Z}$ has no nonzero nilpotent elements, neither does R .
 - (c) Find all nonzero idempotent elements of R .
An element (a, b) in a direct sum is idempotent if and only if each entry is idempotent. In an integral domain such as \mathbf{Z} , the elements 0 and 1 are the only idempotents. The possible idempotents in $\mathbf{Z} \oplus \mathbf{Z}$ are $(0, 0), (1, 0), (0, 1), (1, 1)$ and of these only $(0, 0)$ and $(1, 1)$ are in R , so $(1, 1)$ is the only nonzero idempotent.
 - (d) Find all units of R .
An element (a, b) in a direct sum is a unit if and only if each entry is a unit. Remember that the only units of \mathbf{Z} are ± 1 . Any unit of R is also a unit of $\mathbf{Z} \oplus \mathbf{Z}$, so the possible units are $(1, 1), (-1, -1), (1, -1), (-1, 1)$. All of these belong to R , so this is the set of units of R .

4. (30 pts) (a) State the definition of a prime ideal. In the ring \mathbf{Z} , give an example of an ideal that is prime, and an example of an ideal that is not prime. (Explain why or why not.)

In \mathbf{Z} the ideal $\{0\}$ is a prime ideal since \mathbf{Z} is an integral domain. You can also give the ideal $p\mathbf{Z}$, where p is prime, since we know that in this case $\mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p$ is a field, and every field is an integral domain. The same reasoning shows that $n\mathbf{Z}$ is not prime if n is composite. A direct argument for this just uses the fact that if $n = ab$ for proper factors a and b , the $ab = n \in n\mathbf{Z}$ but neither a nor b belongs to $n\mathbf{Z}$.

(b) State the definition of an integral domain. Give an example of an integral domain, and an example of a ring that is *not* an integral domain. (Explain why or why not.)

The ring \mathbf{Z} of integers is the best known example of an integral domain. I wouldn't even expect an explanation for this example. The solution to part (a) shows that \mathbf{Z}_n is not an integral domain if n is composite. A specific example would be \mathbf{Z}_4 , in which $2 \cdot 2 = 0$ but $2 \neq 0$.

(c) Let I be an ideal of the ring R . Prove the theorem in the text which states that I is a prime ideal of R if and only if R/I is an integral domain.

5. (20 pts) Let R be a subring of S . (a) Show that if I is an ideal of S , then $I \cap R$ is an ideal of R .

Let I be an ideal of S . Then I is a subgroup of S under $+$, and so is R , since it is a subring. We know that the intersection of two subgroups is a subgroup, so I is a subgroup of S and therefore of R .

If $r \in R$ and $x \in I \cap R$, then $x \in I$ and $r \in S$, so $rx \in I$. But $r \in R$ and $x \in R$ implies that $rx \in R$ since R is a subring. Thus $rx \in R$. This shows that $rx \in R \cap I$, so I is an ideal of R .

Alternate proof: Let $\pi : S \rightarrow S/I$ be the projection mapping $\pi(s) = s + I$, for all $x \in S$. We have shown that π is a ring homomorphism. If $i : R \rightarrow S$ is the inclusion mapping, then i is a ring homomorphism since R is a subring. Therefore $\pi i : R \rightarrow S/I$ is a ring homomorphism. Finally, $\ker(\pi i) = \{r \in R \mid r + I = 0 + I\} = \{r \in R \mid r \in I\} = I \cap R$, and therefore $I \cap R$ is an ideal of R .

(b) Prove or disprove: If I is a prime ideal of S then $I \cap R$ is a prime ideal of R .

Let $a, b \in R$ with $ab \in I \cap R$. Thinking of a and b as elements of S , We have $a \in I$ or $b \in I$ because $ab \in I$ and I is a prime ideal of S . Thus $I \cap R$ is a prime ideal of R .

Alternate proof: Using πi in the alternate proof of part (a), we see that $R/(I \cap R)$ is isomorphic to a subring of S/I . If I is a prime ideal of S , then S/I is an integral domain, and this implies that $R/(I \cap R)$ is an integral domain, so $I \cap R$ is a prime ideal of R .

(c) Prove or disprove: If I is a maximal ideal of S then $I \cap R$ is a maximal ideal of R .

Consider the subring \mathbf{Z} of \mathbf{Q} . Since \mathbf{Q} is a field, $\{0\}$ is a maximal ideal of \mathbf{Q} . But $\{0\} \cap \mathbf{Z} = \{0\}$ is not a maximal ideal of \mathbf{Z} . You could prove this by observing that \mathbf{Z} is *not* a field, or simply remark that $\{0\} \subset n\mathbf{Z} \subset \mathbf{Z}$ if $1 < n$.

EXTRA CREDIT:

Let R be a commutative ring with a multiplicative identity 1, and let I and J be proper ideals of R . Show that if there exist $u \in I$ and $v \in J$ with $u + v = 1$, then the direct sum $(R/I) \oplus (R/J)$ is isomorphic to $R/(I \cap J)$. (You may assume that $I \cap J$ is an ideal of R .)

This is the "Chinese remainder theorem" for rings. Define $\phi : R \rightarrow (R/I) \oplus (R/J)$ by $\phi(x) = (x + I, x + J)$, for all $x \in R$. It is straightforward to check that this is a ring homomorphism with kernel $I \cap J$, which shows that $I \cap J$ is an ideal. To show that ϕ is onto, given $(a + I, b + J) \in (R/I) \oplus (R/J)$, let $x = av + bu$. Then $a = au + av$, so $a + I = av + I = x + I$ since $au, bu \in I$. Similarly, $b = bu + bv$, so $b + J = bu + J = x + J$ since $av, bv \in J$. The fundamental homomorphism theorem implies that $R/(I \cap J) \cong (R/I) \oplus (R/J)$.