Problem 1. In the following problems, we investigate the relationship between integral domains and fields.

(a) Prove that every field is an integral domain.

(b) Prove that if R is a finite integral domain, then R is a field. **Hint:** Consider the set function $a : R \to R$ given by multiplication by an element a (it will not be a ring homomorphism). If a is a non-zero-divisor, prove this is an injective function, and so must also be surjective since R has finitely many elements.

(c) Find an example of an integral domain which is not a field.

Proof. **(a)** Let $\mathbb{K}$ be a field, and suppose it contains some non-zero zero divisor $b \in \mathbb{K} \setminus \{0\}$. Then there exists some $a \in \mathbb{K} \setminus \{0\}$ such that $ab = ba = 0$. Since $a, b \in \mathbb{K} \setminus \{0\}$, they are both units and so there exist $a^{-1}, b^{-1} \in \mathbb{K}$ such that $a^{-1}a = bb^{-1} = 1 \implies a^{-1}(ab)b^{-1} = 1 = a^{-1}(0)b^{-1} = 0 \implies 1 = 0$. But then $\mathbb{K} = \{0\}$ which is not a field, a contradiction. Therefore, all non-zero elements are not zero divisors and so $\mathbb{K}$ is a commutative ring with unity and no zero divisors, which is the definition of an integral domain.

(b) Let R be a finite integral domain, and let a be some non-zero zero divisor $a \in R \setminus \{0\}$. We show the mapping $a : R \to R$ via $a(x) = ax$, $\forall x \in R$ is a bijection. For all $x, y \in R$,

> **[1-1]** $a(x) = a(y) \implies ax = ay \implies ax - ay = a(x-y) = 0 \implies x = y$
> otherwise a is a zero divisor, and we get a contradiction.
> **[Onto]** $a : R \hookrightarrow R \implies$ the domain is in bijection with its image $\implies |R| = |a(R)|$
> and since $a(R) \subseteq R$ (the domain is equal to the codomain), we must have that $a(R) = R$.

(This image is just the orbit of a in the canonical multiplicative monoid action of R on itself.) So then for each non-zero zero divisor $a \in R \setminus \{0\}$, $\exists x \in R$ such that $a(x) = ax = 1$. That is, each non-zero zero divisor, which is just all of $R \setminus \{0\}$ is a unit. Therefore, R is a commutative ring with unity and inverses for all non-zero elements, which is the definition of a field.

(c) $\mathbb{Z}$ is an integral domain but not a field.

□

Problem 2. Let I, J be ideals in a commutative ring R such that $I + J = (1)$. Prove that $IJ = I \cap J$.

Proof. $(\subseteq)$ Recall that since I, J are ideals of R, $ir \in I$ and $rj \in J$, $\forall i \in I, \forall j \in J, \forall r \in R$. So then for all $ij \in IJ$, we have that $(i)j \in I$ and $i(j) \in J \implies ij \in I \cap J \implies IJ \subseteq I \cap J$.

$(\supseteq)$ $I + J = \langle 1 \rangle \implies \hat{i} + \hat{j} = 1$ for some $\hat{i} \in I, \hat{j} \in J$. Then for all $a \in I \cap J$, $a = a(1) = (1)a = a(\hat{i} + \hat{j}) = a\hat{i} + a\hat{j} \in IJ + JI = IJ$, since commutativity in R implies $IJ = JI$. Therefore, $I \cap J \subseteq IJ$.

Thus,

$$IJ = I \cap J$$

.

□

Problem 3. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J) = \{i \in R \mid \varphi(i) \in J\}$ is an ideal of R.

Proof. $\forall a,b \in \varphi^{-1}(J),\ \varphi(a),\varphi(b) \in J$ and so $\varphi(a-b) = \varphi(a) - \varphi(b) \in J$. So then $a-b \in \varphi^{-1}(J)$ and $\varphi^{-1}(J) \leq_+ R$.

Next, for any $r \in R$ and any $i \in \varphi^{-1}(J),\ \varphi(ri) = \varphi(r)\varphi(i) \in J$ and $\varphi(ir) = \varphi(i)\varphi(r) \in J$, since J is an ideal of S. So then $ri, ir \in \varphi^{-1}(J)$.

Thus,

$$\text{If } \varphi : R \to S \text{ is a ring homomorphism and } J \text{ is an ideal of } S, \text{ then } \varphi^{-1}(J) \text{ is an ideal of } R.$$

□

We prove some lemmas to be used in some of the next problems.

Lemma 1. *If I,J are ideals of a ring R, then $I+J = \{i+j \mid i \in I, j \in J\}$ is also an ideal of R.*

Proof. $\forall (i_1+j_1),(i_2+j_2) \in I+J,\ (i_1+j_1)-(i_2+j_2) = (i_1-i_2)+(j_1-j_2) \in I+J \implies I+J \leq_+ R$. Next for all $r \in R$ and all $(i+j) \in I+J,\ r(i+j) = ri+rj, (i+j)r = ir+jr \in I+J$ since $ir, ri \in I$ and $rj, jr \in J$. Thus,

$$\text{If } I,J \text{ are ideals of } R, \text{ then } I+J \text{ is an ideal of } R.$$

□

Lemma 2. *If $S \subseteq R$ is a subring of a ring R, then the inclusion mapping $\iota : S \hookrightarrow R$ defined via $\iota(s) = s$ is a ring embedding (an injective ring homomorphism).*

Proof. For all $a,b \in S$,

$$\begin{aligned}
&\iota(a+b) = a+b = \iota(a)+\iota(b)\\
&\iota(ab) = ab = \iota(a)\iota(b)\\
&\iota(1_S) = 1_S = 1_R\\
&\iota(a) = \iota(b) \implies a = b \text{ by definition.}
\end{aligned}$$

□

Problem 4. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of R.

(a) Prove that $\varphi(J) = \{\varphi(j) \mid j \in J\}$ need not be an ideal of S.

(b) Prove that if φ is surjective, then $\varphi(J)$ is an ideal of S.

(c) Prove that if φ is surjective, and $I = \ker\varphi$, then $S \cong R/I$ and if we let $\overline{J} \subseteq R/I$ be the image of $\varphi(J)$ under this isomorphism, then
$$(R/I)/\overline{J} \cong R/(I+J).$$

Proof. **(a)** Consider the inclusion map $\iota : \mathbb{Z} \hookrightarrow \mathbb{R}$ defined by $\iota(n) = n \in R$, $\forall n \in \mathbb{Z}$. This is a ring embedding by **Lemma 2**. Now look at $2 \in 2\mathbb{Z}$, which is a well-known ideal of $\mathbb{Z}$. Well, $\pi \in \mathbb{R}$ but $2\pi = \pi 2 \notin \iota(2\mathbb{Z}) = 2\mathbb{Z}$. So then $\iota(2\mathbb{Z})$ is not an ideal and we see that the ring homomorphic image of an ideal need not be an ideal of the codomain.

(b) For all $\varphi(a), \varphi(b) \in \varphi(J)$ with preimages $a, b \in J$, $\varphi(a) - \varphi(b) = \varphi(a-b) \in \varphi(J)$ since $a - b \in J$. Therefore $\varphi(J) \leq_+ S$. Next, since φ is surjective, for any $s \in S$, $\exists r \in R$ such that $s = \varphi(r)$. So then $s\varphi(a) = \varphi(r)\varphi(a) = \varphi(ra)$ and $\varphi(a)s = \varphi(a)\varphi(r) = \varphi(ar)$ which must both belong to $\varphi(J)$ since $J \subseteq R$ is an ideal $\implies ar, rs \in J$. Therefore, $\varphi(J)$ is an ideal of S. That is, a surjective ring homomorphic image of an ideal is in fact an ideal of the codomain.

(c) φ is surjective, so by the First Isomorphism Theorem $R/\ker\varphi = R/I \cong \varphi(R) = S$ and so $S \cong R/\ker\varphi = R/I$. Let $\psi : R/I \to S$ be this pullback isomorphism. That is,

$$\overbrace{r}^{R} \overset{\varphi}{\mapsto} \overbrace{\varphi(r) = s}^{S} \overset{\psi}{\longleftrightarrow} \overbrace{[r]_I = [r]_{\ker\varphi}}^{I=\ker\varphi} \tag{1}$$

$$\text{So: } \psi(s) = \psi(\varphi(r)) = [r]_I \in R/I, \text{ for each } s = \varphi(r) \in \varphi(R) = S \tag{2}$$

$$\implies \psi(\varphi(j)) = [j]_I \in R/I \text{ for each } j \in J \tag{3}$$

$$\text{Now let: } \overline{J} = \psi(\varphi(J)) = \{\psi(\varphi(j)) = [j]_I \mid j \in J\} \subseteq R/I \tag{4}$$

Recall the Third Isomorphism Theorem. For ideals A, B of a ring R where $A \subseteq B$ is a subset:

$$\text{① } B/A \text{ is an ideal of } R/A \text{ and ② } \frac{(R/A)}{(B/A)} \cong \frac{R}{B}.$$

** Note that in normal rings without unity required, B/A is actually a quotient ring since ideals are always rings. That is: A is an ideal of B if every ideal is a ring. That need not be true if you require rings to have unity and then B/A need not be a quotient ring, but just a set of cosets. However, the resulting quotient is always a quotient ring since the set of cosets (B/A) is an ideal of the quotient ring (R/A). Yet another reason why (a) this coset notation sucks, and (b) this ring definition sucks.**

By **Lemma 1**, $I+J$ is an ideal of R since I, J are ideals of R. Also, $I \subseteq I+J$ is a subset. Well, we can simply compute that $(I+J)/I = \{(i+j)+I \mid (i+j) \in I+J\} = \{j+I = [j]_I \mid j \in J\} = \overline{J}$ by (4).

Therefore, since $I, (I+J)$ are ideals of R with $I \subseteq (I+J)$, by the Third Isomorphism Theorem we have that

$$\text{① } \overline{J} = (I+J)/I \text{ is an ideal of } (R/I) \text{ and ② } \frac{(R/I)}{\overline{J}} = \frac{(R/I)}{(I+J)/I} \cong \frac{R}{(I+J)}.$$

□

Problem 5. Let R be a commutative ring, $a \in R$, and let $f_1(x), \ldots, f_r(x) \in R[x]$.

(a) Prove that $R[x]/(x-a) \cong R$.

(b) Prove the equality of ideals

$$(f_1(x), \ldots, f_r(x), x-a) = (f_1(a), \ldots, f_r(a), x-a).$$

(c) Prove the useful substitution trick

$$R[x]/(f_1(x), \ldots, f_r(x), x-a) \cong R/(f_1(a), \ldots, f_r(a)).$$

Hint: Use part (c) of the previous problem.

We use the telescoping identity for (a). Will do proof later.

Problem 6. If $\Bbbk$ is an algebraic closed field, then the only maximal ideals of $\Bbbk[x]$ are of the form $(x-a)$ where $a \in \Bbbk$. In this problem, we'll see that this is not true when $\Bbbk$ is not algebraically closed.

(a) Use the first isomorphism theorem to show that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

(b) Prove that (x^2+1) is a maximal ideal of $\mathbb{R}[x]$.

Problem 7. Let R be a commutative ring with $0 \neq 1$. In this problem, we will prove that every proper ideal of R is contained in some maximal ideal.

(a) Look up Zorn's Lemma and record it here.

(b) Define $S = \{J \mid J \text{ is a proper ideal of } R \text{ and } J \supseteq I\}$. Explain why S is a partially ordered set (what is the ordering?).

(c) Given a chain C in S, prove that $\bigcap_{J \in C} J$ is an ideal of R (you will use that C is totally ordered), and further that this ideal is in the set S.

(d) Conclude using Zorn's Lemma that S has a maximal element.

Problem 8. Let $\Bbbk$ be a field. In this problem, we will prove that the only maximal ideal of $\Bbbk[[x]]$ is (x), which makes $\Bbbk[[x]]$ a local ring.

(a) Explain why $(x) = \{f \in \Bbbk[[x]] \mid f \text{ has no constant term}\}$.

(b) Compute $\Bbbk[[x]]/(x)$, and then explain why (x) is a maximal ideal.

(c) You may freely use the following result from the optional hint last week: $f \in \Bbbk[[x]]$ is a unit if and only f has a nonzero constant term. Use Proposition 1.41 to show that the only maximal ideal of $\Bbbk[[x]]$ is (x).

Problem 9. Let d be an integer which is not the square of an integer, and consider

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

(a) Prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.

(b) Define a function $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(a+b\sqrt{d}) = a^2 + b^2 d$. Prove that $N(zw) = N(z)N(w)$ and that $N(z) \neq 0$ if $z \neq 0$. This function is often called the norm.

(c) Prove that $\mathbb{Q}(\sqrt{d})$ is a field and is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$ (use N).

(d) Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$.