

**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<sup>1</sup> integral domain, then  $R$  is a field. **Hint:** Consider the set function  $a : R \rightarrow R$  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  $a : R \rightarrow R$  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  $a(R) \subseteq R$ , we must have that  $a(R) = R$ .

(This image is just the orbit of  $a$  in a 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 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  $rz \in J, \forall i \in I, \forall j \in J, \forall r \in R$ . So then for all  $ij \in IJ$ , we have that  $(i)j \in I$  and  $i(j) \in J \implies ij \in I \cap J \implies IJ \cap I \cap J$ .

( $\supseteq$ )  $I + J = \langle 1 \rangle \implies i + j = 1$  for some  $i \in I, j \in J$ . Then for all  $a \in I \cap J$ ,  $a = a(1) = (1)a = a(i + j) = ai + aj = ia + ja = (i + j)a$  □

**Problem 3.** Let  $\varphi : R \rightarrow S$  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  $R$ .

---

<sup>1</sup>meaning  $|R| < \infty$

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

- (a) Prove that  $\varphi(J) = \{\varphi(j) \mid j \in J\}$  need not be an ideal of  $S$ .
- (b) Prove that if  $\varphi$  is surjective, then  $\varphi(J)$  is an ideal of  $S$ .
- (c) Prove that if  $\varphi$  is surjective, and  $I = \ker \varphi$ , then  $S \cong R/I$  and if we let  $\bar{J} \subseteq R/I$  be the image of  $\varphi(J)$  under this isomorphism, then

$$(R/I)/\bar{J} \cong R/(I+J).$$

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

- (a) Prove that  $R[x]/(x-a) \cong R$ .
- (b) Prove the equality of ideals

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

- (c) Prove the useful substitution trick

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

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

**Problem 6.** If  $\mathbb{k}$  is an algebraic closed field, then the only maximal ideals of  $\mathbb{k}[x]$  are of the form  $(x-a)$  where  $a \in \mathbb{k}$ . In this problem, we'll see that this is not true when  $\mathbb{k}$  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  $\mathbb{k}$  be a field. In this problem, we will prove that the only maximal ideal of  $\mathbb{k}[[x]]$  is  $(x)$ , which makes  $\mathbb{k}[[x]]$  a local ring.

- (a) Explain why  $(x) = \{f \in \mathbb{k}[[x]] \mid f \text{ has no constant term}\}$ .
- (b) Compute  $\mathbb{k}[[x]]/(x)$ , and then explain why  $(x)$  is a maximal ideal.

- (c) You may freely use the following result from the optional hint last week:  $f \in \mathbb{k}[[x]]$  is a unit if and only if  $f$  has a nonzero constant term. Use Proposition 1.41 to show that the only maximal ideal of  $\mathbb{k}[[x]]$  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  $N : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}$  by  $N(a + b\sqrt{d}) = a^2 + b^2d$ . 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  $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$ .