Solution 5

PRIME AND MAXIMAL IDEALS, ARITHMETIC OF POLYNOMIALS

1. Let R be a commutative ring. Assume that there exists an ideal $I \subset R$ such that

$$R^\times = R \smallsetminus I \tag{1}$$

   (a) Show that I is a maximal ideal.

   (b) Show that I is the unique maximal ideal in R.

   (c) Conversely, assume that I is the unique maximal ideal of a commutative ring R. Prove that $R^\times = R \smallsetminus I$ holds.

   We call a commutative ring R *local* if there is an ideal $I = \mathfrak{m}_R \subset R$ satisfying (1) (which as just shown is equivalent to asking that $\mathfrak{m}_R$ is the unique maximal ideal of R). The field $R/\mathfrak{m}_R$ is called the *residue field* of the local ring R.

   Solution:

   (a) Let $I \subset J \subset R$ for some ideal J and suppose that $J \neq R$. Then, for each $j \in J$, either $j \in I$ or $j \in R^\times$. Since $j \in R^\times$ implies that $1 \in J$ so that $J = R$, the only possibility is that $j \in I$, so that $J \subset I$ and I is maximal because J was arbitrary.

   (b) Let $J \subset R$ be a maximal ideal, so that $J \neq R$. Then, as observed above, J does not contain units of R. This implies that $J \subset I \neq R$ and by maximality of J we obtain an equality $J = I$.

   (c) Suppose that I is the unique maximal ideal of R. In particular, I is maximal, so it does not contain any unit of R, meaning that $R^\times \subset R \smallsetminus I$. Conversely, assume that $r \in R \smallsetminus I$ and look at the ideal rR. If rR is a proper ideal, then rR is contained in a maximal ideal of R which by assumption implies that $rR \subset I$, a contradiction since $r \notin I$. Hence $rR = R$, so that $1 \in rR$ which means that $r \in R^\times$. This implies that $R^\times \supset R \smallsetminus I$.

2. Let p be a prime number and consider the set

$$\mathbb{Z}_{(p)} = \left\{ x \in \mathbb{Q} : x = \frac{a}{b} \text{ for some } a, b \in \mathbb{Z}, \, p \nmid b \right\}.$$

   (a) Show that $\mathbb{Z}_{(p)}$ is a commutative ring.

   (b) Show that $\mathbb{Z}_{(p)}$ is a local ring. Find its maximal ideal and its residue field.

Solution:

(a) The set $\mathbb{Z}_{(p)}$ is embedded by definition in $\mathbb{Q}$. We check that $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$. Since $p \nmid 1$, we can take $b = 1$ and see that the set $\mathbb{Z}_{(p)}$ contains all the integers. In particular it contains 0 and 1. For every $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Z}_{(p)}$, with $p \nmid b, b'$, the denominators of $\frac{a}{b} - \frac{a'}{b'}$ and $\frac{a}{b}\frac{a'}{b'}$ can both be taken to be bb'. As p is a prime number, $p \nmid bb'$, so that $\frac{a}{b} - \frac{a'}{b'}, \frac{a}{b}\frac{a'}{b'} \in \mathbb{Z}_{(p)}$ and $\mathbb{Z}_{(p)}$ is a ring. It is commutative because $\mathbb{Q}$ is.

(b) If R is a local ring, then $R \setminus R^{\times} = I$ must be an ideal of R by (1). Let us compute $\mathbb{Z}_{(p)}^{\times}$. Consider a fraction $a/b \in \mathbb{Z}_{(p)}$, written with coprime a and b. Since reducing a fraction with denominator not divisible by p gives a fraction with denominator still not divisible by b, we necessarily have $p \nmid b$. Then $a/b \in \mathbb{Z}_{(p)}^{\times}$ if and only if the element $b/a \in \mathbb{Q}$ belongs to $\mathbb{Z}_{(p)}$. Again by coprimality of a and b, this last condition means that $p \nmid a$. Hence

$$\mathbb{Z}_{(p)} \setminus \mathbb{Z}_{(p)}^{\times} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} : a, b \in \mathbb{Z} \text{ are coprime and } p|a \right\}$$
$$= \left\{ \frac{pa'}{b} \in \mathbb{Z}_{(p)} : a, b \in \mathbb{Z} \text{ are coprime, } p \nmid b \right\}$$
$$= \left\{ \frac{p}{1} \cdot x, x \in \mathbb{Z}_{(p)} \right\} = p\mathbb{Z}_{(p)},$$

which is the ideal in $\mathbb{Z}_{(p)}$ generated by $p = \frac{p}{1}$.

The residue field is the ring $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, which we compute by looking at the first isomorphism theorem. Consider the ring homomorphism f defined as the composition of ring homomorphisms

$$f : \mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)} \longrightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}.$$

The kernel of f is seen to be $p\mathbb{Z}$, so that the first isomorphism theorem induces an isomorphism

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{Im}(f).$$

We claim that f is surjective, which will let us conclude that the residue field of $\mathbb{Z}_{(p)}$ is isomorphic to $\mathbb{F}_p$.

In order to prove our claim, let $a/b \in \mathbb{Z}_{(p)}$. We want to prove that $\frac{a}{b} = m + p\frac{a'}{b'}$ for some integers m, a', b' such that $p \nmid b'$. This can be done by noticing that, since p and b are coprime, there exist $\lambda, \mu \in \mathbb{Z}$ such that $1 = \lambda p + \mu b$. Then the decomposition

$$\frac{a}{b} = \frac{a \cdot 1}{b} = \frac{a \cdot (\lambda p + \mu b)}{b} = a\mu + p \cdot \frac{a\lambda}{b}$$

lets us conclude that $a/b + p\mathbb{Z}_{(p)} = f(a\mu)$. Hence f is surjective.

3. Let R be a commutative ring and I, J ideals in R. Define the ideal

$$IJ := (\{ij : i \in I, j \in J\})R.$$

(a) Why is the set $\{ij : i \in I, j \in J\}$ not necessarily an ideal?

(b) Show that $IJ \subset I \cap J$ and find an example in which the inclusion is strict.

(c) Prove that if I and J are coprime, then $I \cap J = IJ$.

Solution:

(a) The reason why the set $\{ij \in R : i \in I, j \in J\}$ is not itself an ideal is that for $i, i' \in I$ and $j, j' \in J$, the element $ij + i'j'$ may not be decomposable as $i_0 j_0$ for some $i_0 \in I$ and $j_0 \in J$. However, notice that if any of the two ideals I and J is principal, then this special situation does not occur. In order to find a counterexample, we need to consider non-principal ideals. For instance, let $R = \mathbb{C}[X_1, X_2, X_3, X_4]$ and $I = (X_1, X_2)$, $J = (X_3, X_4)$. Then $X_1 X_3 + X_2 X_4$ does not belong to $\{ij : i \in I, j \in J\}$, although both $X_1 X_3$ and $X_2 X_4$ belong to this set. Indeed, suppose by contradiction that $X_1 X_3 + X_2 X_4 = ij$ for $i \in I$ and $j \in J$. The total degrees of i and j add up to 2. Necessarily, $i, j \neq 0$, and since the evaluation of all polynomials of I and J on $(X_1, X_2, X_3, X_4) = (0, 0, 0, 0)$ is zero, then i and j are non-constant. This implies that $\deg(i) = \deg(j) = 1$ and moreover we can write $i = \lambda_1 X_1 + \lambda_2 X_2$ and $j = \lambda_3 X_3 + \lambda_4 X_4$, for some $\lambda_u \in \mathbb{C}$, $u \in \{1, 2, 3, 4\}$. Then we obtain an equality

$$X_1 X_3 + X_2 X_4 = \lambda_1 \lambda_3 X_1 X_3 + \lambda_1 \lambda_4 X_1 X_4 + \lambda_2 \lambda_3 X_2 X_3 + \lambda_2 \lambda_4 X_2 X_4$$

in $\mathbb{C}[X_1, X_2, X_3, X_4]$. In particular, the equality of complex numbers $\lambda_2 \lambda_3 = 0$ tells us that $\lambda_2 = 0$ or $\lambda_3 = 0$, but these conclusions are incompatible with the other equalities $\lambda_1 \lambda_3 = 1$ and $\lambda_2 \lambda_4 = 1$, contradiction. Hence $\{ij : i \in I, j \in J\}$ is not an ideal in this case.

(b) For each $i \in I$ and $j \in J$, the element $ij \in R$ must lie in I and J because I and J are ideals. Hence $\{ij : i \in I, j \in J\} \subset I \cap J$, and since $I \cap J$ is an ideal, we can conclude that $IJ \subset I \cap J$. As suggested by the next part, I and J cannot be coprime, so we can consider some example in which $I \subset J$. Then $I \cap J = I$ and we want that multiplication by elements in J makes the ideal I smaller. It is then easy to come up with the following examples:

- $R = \mathbb{Z}/8\mathbb{Z}$, $I = 4\mathbb{Z}/8\mathbb{Z}$, $J = 2\mathbb{Z}/8\mathbb{Z}$. Then $IJ = 8\mathbb{Z}/8\mathbb{Z} = 0$ is the trivial ideal, whereas $I \cap J = I = 4\mathbb{Z}/8\mathbb{Z}$ is not trivial (the quotient R/I being isomorphic to $\mathbb{Z}/4\mathbb{Z} \neq 0$ by exercise 5).
- $R = \mathbb{R}[X]$, $I = X^5 \mathbb{R}[X]$, $J = X^2 \mathbb{R}[X]$. Then $IJ = X^7 \mathbb{R}[X]$ is strictly smaller than $I \cap J = I = X^5 \mathbb{R}[X]$.

(c) Now we suppose that I, J are coprime ideals. In particular one can write $1 = i + j$ for some $i \in I$ and $j \in J$. Let $x \in I \cap J$. Then

$$x = x \cdot 1 = x(i + j) = xi + xj = ix + xj.$$

As $x \in I \cap J$, both ix and xj are in IJ, implying that $x \in IJ$. This proves the equality of ideals, the other inclusion having been proven in part (b).

4. (a) Consider the polynomials $p, q \in \mathbb{Q}[X]$ defined by

$$p := X^3 - \frac{5}{2}X^2 + \frac{3}{2}X \text{ and } q = 2X^2 - X - 3.$$

Compute the Euclidean division of p by q.

(b) Find a single generator of the principal ideal $(p, q)\mathbb{Q}[X] \subseteq \mathbb{Q}[X]$

(c) Let $K = \mathbb{C}(T)$. Compute the Euclidean division in $K[X]$ of

$$f = X^3 + TX^2 - 1 \text{ by } g = (1 + T)X^2 - 1.$$

(d) Using Euclidean division in $\mathbb{F}_3[X]$, where $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ is the field of three elements, check that the ideals $(X^4 + 2X + 1)\mathbb{F}_3[X]$ and $(X^2 + X - 1)\mathbb{F}_3[X]$ are coprime.

Solution:

(a) We compute the Euclidean division by starting with the highest degree and adjusting the lower coefficients, as seen in class:

$$\begin{aligned} X^3 - \frac{5}{2}X^2 + \frac{3}{2}X &= \frac{1}{2}X(2X^2 - X - 3) + \frac{1}{2}X^2 + \frac{3}{2}X - \frac{5}{2}X^2 + \frac{3}{2}X \\ &= \frac{1}{2}X(2X^2 - X - 3) - 2X^2 + 3X \\ &= \left(\frac{1}{2}X - 1\right)(2X^2 - X - 3) - X - 3 + 3X \\ &= \left(\frac{1}{2}X - 1\right)(2X^2 - X - 3) + 2X - 3 \end{aligned}$$

so that we get quotient $\frac{1}{2}X - 1$ and remainder $2X - 3$.

(b) From now on we will omit the ring when writing the ideal generated by some element. Part (a) tells us that

$$\left(X^3 - \frac{5}{2}X^2 + \frac{3}{2}X, 2X^2 - X - 3\right) = (2X^2 - X - 3, 2X - 3) \subset \mathbb{Q}[X].$$

We perform a further Euclidean division:

$$2X^2 - X - 3 = X(2X - 3) + 3X - X - 3 = (X + 1)(2X - 3),$$

so that $\left(X^3 - \frac{5}{2}X^2 + \frac{3}{2}X, 2X^2 - X - 3\right) = (2X - 3) \subset \mathbb{Q}[X].$

4

(c) We use the Euclidean method over the field of functions $\mathbb{C}(T)$.

$$f = X^3 + TX^2 - 1 = \frac{1}{1+T}X((1+T)X^2 - 1) + \frac{1}{1+T}X + TX^2 - 1$$
$$= \left(\frac{1}{1+T}X + \frac{T}{1+T}\right)((1+T)X^2 - 1) + \frac{1}{1+T}X - 1 + \frac{T}{1+T}$$
$$= \left(\frac{1}{1+T}X + \frac{T}{1+T}\right)g + \frac{1}{1+T}X - \frac{1}{1+T}.$$

(d) We compute the Euclidean division of $u := X^4 + 2X + 1$ by $v := X^2 + X - 1$ in $\mathbb{F}_3[X]$:

$$X^4 + 2X + 1 = X^2(X^2 + X - 1) - X^3 + X^2 + 2X + 1$$
$$= (X^2 - X)(X^2 + X - 1) + X^2 - X + X^2 + 2X + 1$$
$$= (X^2 - X + 2)(X^2 + X - 1) - 2X + 2 + X + 1$$
$$= (X^2 - X + 2)(X^2 + X - 1) + 2X.$$

Hence $(X^4 + 2X + 1, X^2 + X - 1) = (X^2 + X - 1, -X) = (X^2 + X - 1, X) = (-1, X) = (-1) = \mathbb{F}_3[X]$, so that the two given ideals are coprime.

5. Let R be a commutative ring and $I \subset R$ an ideal.

   (a) Show that for $J \subset R$ an ideal containing I, there is an isomorphism

   $$(R/I)/(J/I) \xrightarrow{\sim} R/J.$$

   (b) Show that the maximal (resp., prime) ideals of R/I are the ideals J/I where $J \subset R$ is a maximal (resp., prime) ideal containing I.

   Solution:

   (a) Since $I \subseteq J$ and J is the kernel of the canonical projection $p_J : R \longrightarrow R/J$, this projection factors through R/I, i.e., there is a commutative diagram

   where p_I is the canonical projection. The map $f : R/I \longrightarrow R/J$ is surjective because p_J is surjective. Moreover,

   $$\ker(f) = \{r + I, \, r \in R : r + J = J\} = \{r + I, \, r \in J\} = J/I,$$

   so that by the first isomorphism theorem the map f induces a ring isomorphism

   $$\varphi : (R/I)/(J/I) \xrightarrow{\sim} R/J.$$

(b) As seen in class, the ideals of R/I are all J/I where J are ideals of R containing I. Notice that, for such an ideal $I \subset J \subset R$, the ideal J/I is prime (resp., maximal) if and only if $(R/I)/(J/I)$ is an integral domain (resp., a field). The latter condition is equivalent to R/J being an integral domain (resp., a field), because of the isomorphism φ from part (a). Finally, the last condition is equivalent to J being a prime (resp., maximal) ideal in R, which proves the desired statement.

6. Find all the ideals of $\mathbb{Z}/8\mathbb{Z}$. Which are prime? Which are maximal?

Solution: The ideals of $\mathbb{Z}/8\mathbb{Z}$ are $J/8\mathbb{Z}$ where $J \subset \mathbb{Z}$ is an ideal containing $8\mathbb{Z}$. Since the ideals of $\mathbb{Z}$ are all principal, we look for $J = a\mathbb{Z} \subset 8\mathbb{Z}$, which is equivalent to $a|8$. Since a change of sign in a gives the same J (as $-1 \in \mathbb{Z}^\times$), we have the four possibilities $a \in \{1, 2, 4, 8\}$. This gives four ideals $\mathbb{Z}/8\mathbb{Z}$, $2\mathbb{Z}/8\mathbb{Z}$, $4\mathbb{Z}/8\mathbb{Z}$ and $8\mathbb{Z}/8\mathbb{Z} = (0)$. By Exercise 5b), the ideal $J/8\mathbb{Z} \subset \mathbb{Z}/8\mathbb{Z}$ is prime (resp., maximal) if and only if $J \subset \mathbb{Z}$ is prime (resp., maximal). Hence

- The ideal $2\mathbb{Z} \subset \mathbb{Z}$ is prime and maximal, so that $2\mathbb{Z}/8\mathbb{Z} \subset \mathbb{Z}/8\mathbb{Z}$ is a prime and maximal ideal.

- The ideals $\mathbb{Z}, 4\mathbb{Z}, 8\mathbb{Z} \subset \mathbb{Z}$ are neither prime nor maximal, so that the ideals $\mathbb{Z}/8\mathbb{Z}, 4\mathbb{Z}/8\mathbb{Z}, (0) \subset \mathbb{Z}/8\mathbb{Z}$ are neither prime nor maximal.

7. Which of the following ideals of $\mathbb{Z}/4\mathbb{Z}[X]$ are prime? Which are maximal? [*Hint:* quotient ring]

    (a) $(X, 2)(\mathbb{Z}/4\mathbb{Z}[X]) \subset \mathbb{Z}/4\mathbb{Z}[X]$;
    (b) $2(\mathbb{Z}/4\mathbb{Z}[X]) \subset \mathbb{Z}/4\mathbb{Z}[X]$;
    (c) $(X - 1)(\mathbb{Z}/4\mathbb{Z}[X]) \subset \mathbb{Z}/4\mathbb{Z}[X]$.

Solution:

    (a) The surjective ring homomorphism $\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ reducing all classes modulo 2 induces a surjective ring homomorphism

    $$\varphi : \mathbb{Z}/4\mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

    sending $X \mapsto 0$. Writing a general polynomial $f \in \mathbb{Z}/4\mathbb{Z}[X]$ as $f = a + Xg$ for some $a \in \mathbb{Z}/4\mathbb{Z}$ and $g \in \mathbb{Z}/4\mathbb{Z}[X]$, we notice that $\varphi(f) = 0$ if and only if $a \in 2\mathbb{Z}/4\mathbb{Z}$, in which case $f \in (2, X)$. As $\varphi(2) = \varphi(X) = 0$, we deduce that $\ker(\varphi) = (2, X)\mathbb{Z}/4\mathbb{Z}[X]$ and the first isomorphism theorem reads

    $$\mathbb{Z}/4\mathbb{Z}[X]/((2, X)\mathbb{Z}/4\mathbb{Z}[X]) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}.$$

    Since the latter is a field, the ideal $(2, X)\mathbb{Z}/4\mathbb{Z}[X]$ is maximal (and in particular prime).

(b) The ideal $2(\mathbb{Z}/4\mathbb{Z}[X])$ is the kernel of the unique ring homomorphism

$$\mathbb{Z}/4\mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}[X]$$

which sends $X \mapsto X$ and constant elements to their reduction modulo 2. Since this ring homomorphism is surjective, the first isomorphism theorem reads

$$(\mathbb{Z}/4\mathbb{Z}[X])/(2\mathbb{Z}/4\mathbb{Z}[X]) \overset{\sim}{\longrightarrow} \mathbb{Z}/2\mathbb{Z}[X].$$

As $\mathbb{Z}/2\mathbb{Z}[X]$ is an integral domain (because $\mathbb{Z}/2\mathbb{Z}[X]$ is a domain) but not a field, the ideal $2(\mathbb{Z}/4\mathbb{Z}[X])$ of $\mathbb{Z}/4\mathbb{Z}[X]$ is prime but not maximal.

(c) Consider the evaluation at 1, that is, the unique ring homomorphism

$$\mathrm{ev}_1 : \mathbb{Z}/4\mathbb{Z}[X] \longrightarrow \mathbb{Z}/4\mathbb{Z}$$

which is the identity on constant polynomials and sends $X \mapsto 1$. As seen in the Hint to Assignment 3, Exercise 5(d), each polynomial $f \in \mathbb{Z}/4\mathbb{Z}[X]$ can be written as $f = (X-1)g + f(1)$. This tells us that $\ker(\mathrm{ev}_1) = (X-1)\mathbb{Z}/4\mathbb{Z}[X]$ and since ev_1 is surjective, the first isomorphism theorem reads

$$\mathbb{Z}/4\mathbb{Z}[X]/((X-1)\mathbb{Z}/4\mathbb{Z}[X]) \overset{\sim}{\longrightarrow} \mathbb{Z}/4\mathbb{Z},$$

by which we can conclude that $(X-1)\mathbb{Z}/4\mathbb{Z}[X]$ is neither prime neither maximal, as $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

8. Let R_1, R_2 be two commutative rings and $R = R_1 \times R_2$. Let $I \subset R$ be an ideal and define

$$I_1 := \{a \in R_1 : (a,0) \in I\} \subset R_1$$
$$I_2 := \{b \in R_2 : (0,b) \in I\} \subset R_2.$$

(a) Show that I_1, I_2 are ideals in R and that $I = I_1 \times I_2$.

(b) Prove that the ideal I is maximal (resp., prime) if and only if either $I_1 = R_1$ and I_2 is maximal (resp., prime) or $I_2 = R_2$ and I_1 is maximal (resp., prime).

Solution:

(a) Clearly, $0 \in I_1$ as $(0,0) \in I$ since I is an ideal. For each $i, i' \in I_1$, we know that $(i,0), (i',0) \in I$ so that

$$(i,0) - (i',0) = (i-i',0) \in I$$

and $i - i' \in I_1$. Finally, for $r \in R_1$, we know that

$$(i,0) \cdot (r,0) = (ir,0) \in I,$$

which implies that $ir \in I_1$. This concludes the proof that I_1 is an ideal. The analog argument on the second component proves that I_2 is an ideal. We prove the equality $I = I_1 \times I_2$ by checking the two inclusion:

7

- For each $i_1 \in I_1$ and $i_2 \in I_2$, by definition we know that $(i_1, 0), (0, i_2) \in I$. Then $(i_1, i_2) = (i_1, 0) + (0, i_2) \in I$. This proves that $I \supset I_1 \times I_2$.
- Conversely, let $(i_1, i_2) \in I$. Since I is an ideal, it contains both $(i_1, i_2) \cdot (1, 0) = (i_1, 0)$ and $(i_1, i_2) \cdot (0, 1) = (0, i_2)$, which implies that $i_1 \in I_1$ and $i_2 \in I_2$, i.e., $(i_1, i_2) \in I_1 \times I_2$. This prooves that $I \subset I_1 \times I_2$.

(b) Notice that combining the two natural projections $R_i \longrightarrow R_i/I_i$ we get a surjective ring homomorphism

$$R = R_1 \times R_2 \longrightarrow R_1/I_1 \times R_2/I_2 \tag{2}$$

with kernel $I_1 \times I_2 = I$ by part (a). Hence $R/I \cong R_1/I_1 \times R_2/I_2$ by the first isomorphism theorem. Notice that if $I_2 = R_2$, then this isomorphism tells us that $R/I \cong R_1/I_1$, so that I is prime (resp., maximal) if and only if I_1 is prime (resp., maximal), because this condition is equivalent to the quotient ring being a domain (resp., a field). Similarly, for $I_1 = R_1$ we get that I is prime (resp., maximal) if and only if I_2 is prime (resp., maximal).

In order to conclude, we need to check that either $I_1 = R_1$ or $I_2 = R_2$ whenever I is prime. This is because of the isomorphism $R/I \cong R_1/I_1 \times R_2/I_2$ that we proved above. Indeed, the two rings R_1/I_1 and R_2/I_2 cannot be both non-trivial, because otherwise their product would contain the two non-zero elements $(1, 0)$ and $(0, 1)$ with product 0, which is a contradiction with R/I being a domain (as I is assumed to be prime). Hence either $R_1/I_1 = 0$ or $R_2/I_2 = 0$, that is, either $I_1 = R_1$ or $I_2 = R_2$.