Problem Set 11
solutions

Problem 1. Let $I = (2, x)$ in $R = \mathbb{Z}[x]$.

(5.1) Show that $\mathfrak{m} = (2, x)$ is a maximal ideal.

Proof. Consider the ring homomorphism $\mathrm{ev}_0 : \mathbb{Z}[x] \to \mathbb{Z}$ given by evaluation at 0. On the one hand, this map is surjective, as any $n \in \mathbb{Z}$ can be obtained by evaluating the constant polynomial n: $\mathrm{ev}_0(n) = n$. The kernel of ev_0 is the set of polynomials with zero constant term, which are the multiples of x, so $\ker(\mathrm{ev}_0) = (x)$. By the First Isomorphism Theorem for rings, we conclude that

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}.$$

Moreover, under this isomorphism $I/(x)$ corresponds to $\mathrm{ev}_0(I)$. Since I is the set of all polynomials with even constant term, we conclude that $I/(x)$ corresponds to $\mathrm{ev}_0(I) = (2)$ under the isomorphism

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$$

above. Thus

$$(\mathbb{Z}[x]/(x))/(I/(x)) \cong \mathbb{Z}/(2).$$

By the Third Isomorphism Theorem for rings,

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/(x))/(I/(x)).$$

Therefore,

$$\mathbb{Z}[x]/I \cong \mathbb{Z}/(2). \quad \square$$

Now note that $\mathbb{Z}/(2)$ is a field, and thus I must be a maximal ideal.

(5.2) Show that $(2, x)$ is not a principal ideal.

Proof. Suppose by way of contradiction that $(2, x) = (f)$ for some $f \in \mathbb{Z}[x]$. Since $2 \in (f)$, we have $2 = fg$ for some $g \in \mathbb{Z}[x]$. Since $\mathbb{Z}$ is a domain,

$$0 = \deg 2 = \deg(fg) = \deg f + \deg g,$$

and since $f, g \neq 0$ we conclude that

$$\deg(f) = \deg(g) = 0.$$

Hence f and g are constant polynomials, say $f = p$ and $g = q$ with $p, q \in \mathbb{Z}$. Therefore, $2 = pq$ in $\mathbb{Z}$, and since 2 is a prime integer either $p = \pm 1$ and $q = \pm 2$ or $p = \pm 2$ and $q = \pm 1$. We conclude that either $(f) = R$ or $(f) = (2)$. We will show that both of these are impossible.

Suppose that $I = (2, x) = R$. Then $1 \in (2, x)$, so there exist $u, v \in \mathbb{Z}[x]$ such that

$$1 = 2u + xv.$$

The constant term of the polynomial 1 is the integer 1, while the constant term of $2u + xv$ is twice the constant term of u, and thus even. This is a contradiction, so $(2, x) \neq R$.

If $I = (2, x) = (2)$, then $x \in (2)$, and thus $x = 2h$ for some polynomial $h \in \mathbb{Z}[x]$. Again this leads to a contradiction: every nonzero coefficient of the polynomial x is odd, while every nonzero coefficient of the polynomial $2h$ is even.

We conclude that $(2, x)$ cannot be principal. $\square$

Problem 2. Show that every finite domain must be a field.

Proof. Let R be a finite domain, and consider any nonzero element $x \in R$. Since R is finite, there are only finitely many elements of the form x^n with $n \geqslant 0$. In particular, there exist $n > m$ such that $x^n = x^m$. Thus by the cancellation rule, we have

$$x^m \cdot x^{n-m} = x^m \implies x^{n-m} = 1.$$

Note that $a = n - m > 0$ and $x^a = 1$. In particular, x is a unit, with inverse x^{a-1}. We conclude that R is a field. □

Problem 3. Consider the ring $R = \mathbb{Z}[x]$ and the ideal $I = (3, x^3 + x + 1)$.

(2.1) Show that $R/I \cong (\mathbb{Z}/3)[x]/(x^3 + x + 1)$.

Proof. Using the Third Isomorphism Theorem, we have

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/(3))/(x^3 + x + 1).$$

Now consider the map quotient map $\pi\colon \mathbb{Z} \to \mathbb{Z}/3$, and let

$$\varphi\colon \mathbb{Z}[x] \longrightarrow (\mathbb{Z}/3)[x]$$

be the ring homomorphism defined by

$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = \pi(a_0) + \pi(a_1)x + \cdots + \pi(a_n)x^n.$$

A polynomial is in $\ker(\varphi)$ if and only if all its coefficients are multiples of 3, and thus $\ker(\varphi) = (3)$. Moreover, φ is surjective by construction. By the First Isomorphism Theorem, we conclude that

$$\mathbb{Z}[x]/(3) \cong (\mathbb{Z}/3)[x].$$

Therefore,

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}/3)[x]/(x^3 + x + 1). \quad \square$$

(2.2) Find, with proof, all the ideals of R that contain I.

Proof. By the Lattice Isomorphism Theorem, the ideals of $(\mathbb{Z}/3)[x]/(x^3 + x + 1)$ correspond to the ideals of $(\mathbb{Z}/3)[x]$ that contain $x^3 + x + 1$. Since $\mathbb{Z}/3$ is a field, $\mathbb{Z}/3[x]$ is a PID. Given any $f \in \mathbb{Z}/3[z]$, $(f) \supseteq (x^3 + x + 1)$ if and only if f divides $x^3 + x + 1$.

The ring $\mathbb{Z}/3$ is a field, and over $\mathbb{Z}/3$ the polynomial $x^3 + x + 1$ factors as

$$x^3 + x + 1 = (x - 1)(x^2 + x - 1).$$

The polynomial $x^2 + x - 1$ has no roots in $\mathbb{Z}/3$, which we can check by explicitly evaluating it at all the three elements of $\mathbb{Z}/3$. Hence, by degree considerations, $x^2 + x - 1$ must be irreducible, as any factor would have degree 1 and lead to a root.

Thus the ideals of $\mathbb{Z}/3[x]$ that contain $x^3 + x + 1$ are (1), $(x^3 + x + 1)$, $(x - 1)$ and $(x^2 + x - 1)$. This gives 4 ideals of $\mathbb{Z}[x]$ that contain I: $\mathbb{Z}[x]$, I, $(3, x - 1)$ and $(3, x^2 + x + 1)$. □

Problem 4. Let R be a commutative ring. Show that every proper ideal $I \neq R$ is contained in some maximal ideal of R.

Proof. Fix a ring R and a proper ideal I. Let

$$S = \{J \text{ proper ideal in } R \mid J \supseteq I\}.$$

This set is partially ordered with the inclusion order $\subseteq$. We claim that Zorn's Lemma applies to S. First, S is nonempty, since it contains I. Now consider a chain of proper ideals in R, say $\{J_i\}_i$, all of which contain I. Now we claim that

$$J := \bigcup_i J_i$$

is an ideal as well. All the J_i are nonempty, so J is nonempty. Moreover, giving $a, b \in J$, and $r \in R$, note that $a \in J_x$ for some index x and $b \in J_y$ for some index y. Since $\{J_i\}_i$ is a totally ordered set, we have $J_x \subseteq J_y$ or $J_y \subseteq J_x$. Assume without loss of generality that $J_y \subseteq J_x$, so that $a, b \in J_x$. Since J_x is an ideal, we have $a - b \in J_x$ and $ra \in J_x$. We conclude that $a - b, ra \in J$, and thus J is an ideal.

Moreover, all the J_i are proper ideals, so $1 \notin J_i$ for all i. We conclude that $1 \notin J$ and thus $J \neq R$. Since each $J_i \supseteq I$, we conclude that $J \supseteq I$. Thus we have checked that $J \in S$. Now this ideal $J \in S$ is an upper bound for our chain $\{J_i\}_i$, and thus Zorn's Lemma applies to S. We conclude that S has a maximal element.

There is one subtle point missing: we have shown that there is a maximal element M in S containing I, but we have yet to show that this maximal element is a maximal ideal of R. Finally, suppose that L is an ideal in R with $L \supseteq M$. Since M contains J, so does L. If $L \in S$, by the maximality of M we must have $L = M$. Since L already satisfies $L \supseteq J$, if $L \notin S$ then we must have $L = R$. We conclude that M is a maximal ideal of R. □

Problem 5. Let R be a commutative ring. We say that R is noetherian if it satisfies the following ascending chain condition: for any ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there exists a positive integer n such that $I_n = I_{n+k}$ for all positive integers k; that is, the ascending chain stabilizes. Prove that a ring R is noetherian if and only if every ideal of R is finitely generated.

Proof. ($\Leftarrow$): Suppose every ideal of R is finitely generated, and consider an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots .$$

Let

$$J = \bigcup_{k=1}^{\infty} I_k,$$

which is an ideal by the previous problem. By assumption, J is finitely generated, say $J = (a_1, ..., a_\ell)$. For each index $1 \leqslant i \leqslant \ell$, the element a_i is in I_{k_i} for some natural number k_i. Set

$$k = \max\{k_1, \ldots, k_\ell\},$$

and note that $I_{k_i} \subseteq I_k$ for all i. Then $a_1, \ldots, a_\ell \in I_k$, and hence $J \subseteq I_k$. But $I_k \subseteq J$, so

$$I_k = I_{k+1} = \cdots = I_n$$

for all $n \geqslant k$, and the chain stops. Thus R is noetherian.

($\Rightarrow$): Suppose that there is an ideal I of R that is not finitely generated. Let $I_0 = 0 = (0)$. Since I is not finitely generated, then $I \neq I_0$, and so there is an element $a_1 \in I \setminus I_0$. Let $I_1 = (a_1)$; then $I_0 \subsetneq I_1$, and $I_1 \neq I$. Suppose by induction that we have constructed $I_j = (a_1, ..., a_j) \subseteq I$ such that

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_j.$$

Since I_j is finitely generated, $I_j \neq I$, so there is an element $a_{j+1} \in I \setminus I_j$. Set $I_{j+1} = (a_1, ..., a_{j+1})$. then

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_{j+1}$$

and $I_{j+1} \subseteq I$. We can thus construct an infinite ascending chain of ideals, so R is not noetherian.

□