Problem Set 12

Due Thursday, December 4

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

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

(a) 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.

(b) 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. □

Problem 2. Let I and J be ideals of a commutative ring R with $1 \neq 0$. You can use without proof that $I + J$, $I \cap J$, and IJ are ideals of R.

(a) Show that $IJ \subseteq I \cap J$.

Proof. Recall that

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \geqslant 0, a_i \in I, b_i \in J \right\}.$$

Given $a \in I$ and $b \in J$, since J is an ideal we have $ab \in J$, and since I is an ideal we have $ab \in I$. We conclude that $ab \in I \cap J$. Moreover, $I \cap J$ is an ideal and thus closed for sums, so for any $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$ we must then have

$$\sum_{i=1}^{n} a_i b_i \in IJ.$$

Thus $IJ \subseteq I \cap J$ always holds. □

(b) Give an example where $IJ \neq I \cap J$.

Proof. Consider the ring $R = k[x]$, where k is any field, and let $I = J = (x)$. Then $I \cap J = I = (x)$, but $IJ = I^2 = (x^2) \neq I \cap J$. □

(c) Suppose that $I + J = R$. Show that $IJ = I \cap J$.

Proof. If $I + J = R$, then there exist $i \in I$ and $j \in J$ such that $i + j = 1$. Let $\alpha \in I \cap J$, then $\alpha = \alpha \cdot 1 = \alpha \cdot (i + j) = ai + aj \in IJ$ and thus it follows that $I \cap J \subseteq IJ$ under the given hypotheses. □

(d) Suppose m and n are distinct maximal ideals of a commutative ring R. Prove that $mn = m \cap n$.

Hint: First consider $m + n$.

Proof. First note that $m+n$ is an ideal, and contains both m and n. Hence, $m+n$ properly contains both (as $m \neq n$), so we must have $m+n=R$. We conclude that $m \cap n = mn$. □

(e) Suppose that $I+J=R$. Show that there is a ring isomorphism $R/(I\cap J) \cong R/I \times R/J$.

Proof. Let $f\colon R \to R/I \times R/J$ be defined by

$$f(r) = (r+I, r+J).$$

This is a ring homomorphism:

- $f(r+s) = (r+s+I, r+s+J) = (r+I, r+J) + (s+I, s+J) = f(r)+f(s)$
- $f(rs) = (rs+I, rs+J) = (r+I, s+I)(r+J, s+J) = f(r)f(s)$.
- $f(1_R) = (1+I, 1+J) = 1_{R/I\times R/J}$.

Note that

$$\ker(f) = \{r \in R \mid r+I = 0+I \text{ and } r+J = 0+J\} = \{r \in R \mid r \in I \text{ and } r \in J\} = I \cap J.$$

Moreover, we claim that f is surjective. Since $I+J=R$, there exist $i \in I$ and $j \in J$ such that $i+j=1$. Set $z := rj+si$. Now given any $(r+I, s+J)$, note that $si, ri \in I$ and $rj, sj \in J$, so

$$z+I = rj+si+I = rj+I = r(1-i)+I = r-ri+I = r+I$$

and

$$z+J = rj+si+J = si+J = s(1-j)+J = s-sj+J = s+J.$$

Thus

$$(r+I, s+J) = (z+I, z+J) = f(z).$$

By the UMP of quotient rings there is a well-defined ring homomorphism

$$\overline{f} : R/(I\cap J) \to R/I \times R/J$$

given by

$$\overline{f}(r+I\cap J) = (r+I, r+J).$$

Moreover, its kernel is $\{0\}$, since $\ker f = I \cap J$, and $\overline{f}$ is surjective since f is surjective. This shows $\overline{f}$ is an isomorphism. □

Problem 3. Let R be a commutative ring. Prove[1] that the set of prime ideals of R has a minimal element with respect to inclusion.

Proof. Let A be the collection of all prime ideals of R. Make A into a poset by declaring $p \leq q$ if and only if $p \supseteq q$. The axioms of a poset are easy to verify. We show the hypotheses of Zorn's Lemma are met.

Since $R \neq 0$, it has at least one maximal ideal, and every maximal ideal is prime. This shows that A is nonempty.

Let B be any totally ordered subset of A. Given the definition of $\leq$, this means that for $p, q \in B$, either $p \supseteq q$ or $q \supseteq p$. If B is empty, then any element of A serves as an upper bound of it for $\leq$.

[1] Note: (0) is not prime unless R is a domain.

Assume B is non-empty, and consider $I = \bigcap_{p \in B} B$. We claim I is a prime ideal, and hence is in A. As stated in class, an arbitrary intersection of ideals is an ideal, and thus it remains to show I is a prime ideal. Since B is nonempty, I is a proper ideal. (Note that the empty intersection is R: this is only place where B being nonempty is used.) Pick $x, y \in R \setminus I$. Then $x \notin p$ for some $p \in B$ and $y \notin q$ for some $q \in B$. Since B is totally ordered, $p \supseteq q$ or $q \supseteq p$, and thus either $x, y \notin q$ or $x, y \notin p$ and hence, since p and q are prime ideals, we have $xy \notin q$ or $xy \notin p$. Either way, $xy \notin B$. This proves I is a prime ideal. Clearly, $p \supseteq I$ for all $p \in B$ and so I is an upper bound of B in A for $\leq$.

We may thus apply Zorn's element, which states that A has a maximal element for $\leq$. That is, there exists a prime ideal p such that if $p \supseteq q$ for another prime ideal q, then $p = q$. □

For the remaining problem, you can use the following theorem, to be covered next Monday.
THEOREM: Let R be a commutative ring, and $g = a_n x^n + \cdots + a_1 x + a_0$ a polynomial in $R[x]$ with a_n a unit in R. Then for any $f \in R[x]$, there exists a unique pair of polynomials $q, r \in R[x]$ such that

- $f = qg + r$, and
- $r = 0$ or $\deg(r) < \deg(g)$.

DEFINITION: Let R be a commutative ring, and $f \in R[x]$ a polynomial. We say that $r \in R$ is a **root** of f if $\mathrm{ev}_r(f) = 0$.

Problem 4. Let R be a commutative ring and $f \in R[x]$.

(a) Show that if $r \in R$ is a root of f, then f is a multiple of the polynomial $x - r$ in $R[x]$.

Proof. By the given Theorem, we may write $f = (x - r)q + p$ for some polynomial $q \in R[x]$ and some $s \in R[x]$ such that $\deg(s) = 0$ or $s = 0$; i.e., either way, s is a constant polynomial. We have

$$\mathrm{ev}_r(f) = \mathrm{ev}_r(q(x - r) + s) = \mathrm{ev}_r(q)\mathrm{ev}_r(x - r) + \mathrm{ev}_r(s) = \mathrm{ev}_r(q) \cdot 0 + s = s,$$

and thus if r is a root, $s = \mathrm{ev}_r(f) = 0$, so $f = (x - r)q$, showing that f is a multiple of $x - r$. □

(b) Show that if R is an integral domain and $\deg(f) = d$, then f has at most d roots.

Proof. We will show that if f has at least d roots in R, then $\deg(f) \geq d$. We proceed by induction on d. If $d = 1$, then we can write $f = ax + b$, and if $ar + b = 0 = ar' + b$, then $a(r - r') = 0$ implies $r - r' = 0$, so $r = r'$, and thus f has at most one root.

Now suppose the claim is true for polynomials with at least $d - 1$ roots, and suppose that f has roots $r_1, \ldots, r_d \in R$, with $r_i \neq r_j$ for all $i \neq j$. By part (a) we can write $f = q(x - r_d)$. For $i = 1, \ldots, d - 1$, we have

$$0 = \mathrm{ev}_{r_i}(f) = \mathrm{ev}_{r_i}(q)\mathrm{ev}_{r_i}(x - r_d),$$

and $\mathrm{ev}_{r_i}(x - r_d) = r_i - r_d \neq 0$, so $\mathrm{ev}_{r_i}(q) = 0$ using that R is an integral domain. Thus, q is a polynomial with at least $d - 1$ roots, namely $r_1, \ldots, r_{d-1}$, and so by the induction hypothesis, $\deg(q) \geq d - 1$. Then, by a previous exercise, since R is a domain, we have

$$\deg(f) = \deg(q) + \deg(x - r) \geq d.$$

This completes the induction.

To get the given statement, note that if $\deg(f) = d$ and f does not at most d roots, then f has at least $d + 1$ roots, contradicting what what we just showed. □

(c) Give an example of a polynomial f over a commutative ring R that has more than $\deg(f)$ roots in R.

Proof. There are many examples, e.g., $x^2 - [1]$ has four roots in $(\mathbb{Z}/3 \times \mathbb{Z}/3)[x]$, namely $([1],[1]),([1],[2]),([2],[1]),([2],[2])$. □