Homework 6

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Friday, March 8th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. Recall: an ideal $P \neq R$ in a commutative ring R is prime if $ab \in P$ implies $a \in P$ or $b \in P$.

   a) Prove that P is prime if and only if R/P is a domain.
   b) Use the first isomorphism theorem to show that the ideals (x) and $(2, x)$ in $\mathbb{Z}[x]$ are prime ideals.[1][2]
   c) Show that the ideal $(4, x)$ in $\mathbb{Z}[x]$ is not prime.
   d) Show that the ideal $(2, \sqrt{10})$ in $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ is prime.
   e) Is the ideal (2) in $\mathbb{Z}[i]$ a prime ideal?

(a) Suppose that $P \neq R$ is not prime. Then, there are $a, b \notin P$ with $ab \in P$. The elements $a + P, b + P$ are nonzero in R/P, but $(a + P)(b + P) = ab + P = 0 + P$ is the zero element in R/P, so R/P is not a domain. The converse is similar.

(b) First, we claim that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. There is a homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ given by evaluation at zero. The kernel of this consists of polynomials with zero constant term, which is just the multiples of x, i.e., (x). This map is surjective, since any integer can be the value-at-zero of an integer polynomial. By the first isomorphism theorem, the claim is shown. Now, since $\mathbb{Z}$ is a domain, by the previous part, (x) is prime. Second, we claim that $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. There is a homomorphism $\mathbb{Z}[x] \to \mathbb{Z}_2$ given by evaluation at zero, taken modulo 2. The kernel of this consists of polynomials with even constant term, which we have seen in class is $(2, x)$. This map is surjective, since the value-at-zero of an integer polynomial can be either even or odd. By the first isomorphism theorem, the claim is shown. Now, since $\mathbb{Z}_2$ is a domain, by the previous part, $(2, x)$ is prime.

(c) We need only note that $2 \notin (4, x)$, but $2 \cdot 2 \in (4, x)$.

(d) We claim first that $a + b\sqrt{10} \in (2, \sqrt{10})$ if and only if a is even. Indeed,

$$\begin{aligned}(2, \sqrt{10}) &= \{2(a_1 + b_1\sqrt{10}) + \sqrt{10}(a_2 + b_2\sqrt{10}) \mid a_1, a_2, b_1, b_2 \in \mathbb{Z}\} \\ &= \{(2a_1 + 10b_2) + (2b_1 + a_2)\sqrt{10} \mid a_1, a_2, b_1, b_2 \in \mathbb{Z}\} \\ &= \{2a' + b'\sqrt{10} \mid a', b' \in \mathbb{Z}\}.\end{aligned}$$

Now, given two elements $a + b\sqrt{10}, c + d\sqrt{10}$ *not* in $(2, \sqrt{10})$, we know that a, c are odd. Then,

$$(a + b\sqrt{10})(c + d\sqrt{10}) = (ac + 10bd) + (ad + bc)\sqrt{10}$$

has $ac + 10bd$ odd, so the product is again not in $(2, \sqrt{10})$. We conclude that the ideal is prime.

[1]Hint: For the first one, consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ "evaluate at zero".
[2]Reminder: $(2, x)$ refers to the ideal generated by 2 and x.

(e) Not prime! Observe that $(1+i)(1-i) = 1 - i^2 = 2$. However, $1+i$ and $1-i$ are not multiples of 2 in $\mathbb{Z}[i]$. This needs to be checked; we can check it by computing $2(a+bi) = (2a)+(2b)i$, so the real coefficient of an element in (2) must be even, which is not the case of $1 \pm i$.

2. We say that a proper ideal I in a ring R is **maximal** if whenever $I \subsetneq J$ for some ideal J, we have $J = R$. For the next problems, assume R is a commutative ring and I is an ideal of R.
   (a) Prove that if I is a maximal ideal and $a \notin I$ then $a + I$ is a unit in R/I.
   (b) Prove that I is a maximal ideal if and only if R/I is a field.[3]
   (c) Use the First Isomorphism Theorem to show that the non-principal ideal $(2, x)$ in $\mathbb{Z}[x]$ is a maximal ideal.[4]
   (d) Show that the ideal $(4, x)$ in $\mathbb{Z}[x]$ is not maximal.
   (e) Show that the ideal $(2, \sqrt{10})$ in $\mathbb{Z}[\sqrt{10}] := \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ is maximal.
   (f) Show that $I := \{a + bi \ : \ 3 \mid a \text{ and } 3 \mid b\}$ is a maximal ideal in $\mathbb{Z}[i]$.[5]

(a) Suppose that I is maximal, and let $a \notin I$. Then $I \subsetneq (a, I)$, so that $(a, I) = R$ by maximality. Then in particular $1_R \in (a, I)$. Hence, there must exist $i \in I$ and $r_1, r_2 \in R$ such that $1 = r_1 a + r_2 i$. Therefore, in R/I we have

$$[1] = [r_1 a + r_2 i] = [r_1 a] + [0] = [r_1][a],$$

so $[a] \in R/I$ is a unit.

Now suppose $[a]$ is a unit in R/I for every $a \notin I$. Suppose $I \subsetneq J$ for some ideal J, and let $a \in J \setminus I$. Then $[a] = a + I \in R/I$ is a unit, so there is some $r \in R$ with $[r][a] = 1$. Therefore, $ra + I = 1 + I$, so that $1 \in J$ since $(a, I) \subseteq J$ and $1 \in (a, I)$. Then $J = R$. Since J was an arbitrary ideal containing I, we have that I is maximal.

(b) If I is maximal, note that the nonzero elements of R/I are of the form $a + I$ where $a \notin I$. Then by the first problem, all nonzero elements of R/I are units, which means that R/I is a field. On the other hand, if I is not maximal, then there is some $I \subsetneq J$ where $J \neq R$. In particular, pick $a \in J$ such that a is not in I. Then $[a]$ is not a unit in R/I, but since $a \notin I$, $[a]$ is also nonzero. Then R/I is not a field since it has a nonzero element which is not a field.

(c) Note that there is a homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2$ given by evaluation at 0, taken modulo 2. The kernel of ϕ consists of all polynomials with even constant term, which we have seen in class is the ideal $(2, x)$. The map ϕ is surjective, since the value-at-zero of an integer polynomial can be either even or odd. By the First Isomorphism Theorem, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. Now, since $\mathbb{Z}_2$ is a field, by the previous part, $(2, x)$ is a maximal ideal.

[3]Remark: Perhaps surprisingly, both directions of this "if and only if" are useful.

[4]Hint: Consider the homomorphism $f\colon \mathbb{Z}[x] \to \mathbb{Z}_2$ given by $f(x) \mapsto [f(0)]_2$

[5]Hint: If $r + si \notin I$, then $3 \not| r$ or $3 \not| s$. Show that 3 does not divide $r^2 + s^2 = (r + si)(r - si)$. Then show that and ideal containing $r + si$ and I also contains 1.

(d) There is a surjective ring homomorphism ϕ given by $f(x) \mapsto [f(0)]_4$, which by the previous argument has a kernel of $(4, x)$. By the First Isomorphism Theorem $\mathbb{Z}[x]/(4, x) \cong \mathbb{Z}_4$, which is not a field, so $(4, x)$ is not a maximal ideal. (We could instead note that $(4, x) \subsetneq (2, x)$ which is not all of $\mathbb{Z}[x]$ so $(4, x)$ is not maximal.)

(e) We claim first that $a + b\sqrt{10} \in (2, \sqrt{10})$ if and only if a is even. Indeed,

$$\begin{aligned}(2, \sqrt{10}) &= \{2(a_1 + b_1\sqrt{10}) + \sqrt{10}(a_2 + b_2\sqrt{10}) \mid a_1, a_2, b_1, b_2 \in \mathbb{Z}\} \\ &= \{(2a_1 + 10b_2) + (2b_1 + a_2)\sqrt{10} \mid a_1, a_2, b_1, b_2 \in \mathbb{Z}\} \\ &= \{2a' + b'\sqrt{10} \mid a', b' \in \mathbb{Z}\}.\end{aligned}$$

Now, given two elements $a + b\sqrt{10}, c + d\sqrt{10}$ *not* in $(2, \sqrt{10})$, we know that a, c are odd. Then,

$$(a + b\sqrt{10})(c + d\sqrt{10}) = (ac + 10bd) + (ad + bc)\sqrt{10}$$

has $ac + 10bd$ odd, so the product is again not in $(2, \sqrt{10})$. Now suppose $I \subsetneq J$. Then there is an element $a + b\sqrt{10}$ in J which is not in I. By the previous argument, a must be odd. But now note that there is some a_2 such that a_2 is even and $a - a_2 = 1$. Note that $a_2 + b\sqrt{10}$ must be in I by the previous argument, since a_2 is even. Since $I \subset J$ it is also in J. Then since J is closed under addition $a + b\sqrt{10} - a_2 - b\sqrt{10} = 1 \in J$ and $J = R$. Since J was an arbitrary ideal containing I, I is maximal.

Alternatively, note that $(2, \sqrt{10}) = \ker \phi$, where $\phi : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}_2$ is given by $a + b\sqrt{10} \mapsto [a]_2$. Then, since ϕ is surjective, the ideal $(2, \sqrt{10})$ is maximal.

(f) Let $I \subsetneq J$, so that there is some $r + si \in J$ which is not in I. If $r + si \notin I$, then $3 \nmid r$ or $3 \nmid s$. Then 3 does not divide $r^2 + s^2 = (r + si)(r - si)$, since if it divides r, then it divides r^2 but not s or s^2 (and similarly if it divides s). If it does not divide either r or s then r, s are 1 or 2 $\pmod 3$. Then $r^2 + s^2$ is 2 $\pmod 3$, so cannot be divisible by 3. Now note that $r^2 + s^2 \notin J$, and either $r^2 + s^2 \equiv 2 \pmod 3$ (if 3 doesn't divide either r or s), or $r^2 + s^2 \equiv 1 \pmod 3$ (if 3 divides only one of r or s). In the second case, there is some $n \in \mathbb{Z}$ such that $r^2 + s^2 - 3n = 1$. In particular, $(r^2 + s^2) - (3n + 0i) = 1$, and the first term is clearly in J, and the second term is clearly in I (so also in J), so 1 is in J and $J = R$. Now suppose $r^2 + s^2 = 2 \pmod 3$, so that 3 does not divide r or s. Then $r^2 \equiv s^2 \equiv 1 \pmod 3$, so there is some n_1, n_2 such that $r^2 - 3n_1 = 1$ and $s^2 - 3n_2 = 1$. Then $r^2 + s^2 - (3(n_1 + n_2) + 0i) = 1$, which is again in J, so that $J = R$.

3. Polynomial rings in *many* variables. Let $R_n = \mathbb{Q}[x_1, x_2, \ldots, x_n]$ is a polynomial ring in variables $x_1, x_2, \ldots, x_n$; that is it contains all polynomials in finite terms that involve these variables.

(a) Let $f_1, f_2, \ldots, f_k$ be polynomials in R_n. Prove that the set

$$\langle f_1, f_2, \ldots f_k\rangle := \{g_1 f_1 + g_2 f_2 + \ldots + g_k f_k \mid g_1, g_2, \ldots, g_n \in R_n\}$$

is an ideal of R_n.

(b) Consider the ring homomorphism

$$\varphi : R_4 \to \mathbb{Q}[t_1, t_2], \varphi(x_1) = t_1^3,\ \varphi(x_2) = t_1^2 t_2,\ \varphi(x_3) = t_1 t_2^2,\ \varphi(x_4) = t_2^3. \tag{1}$$

Explain why the above description fully determines $\varphi(f)$ for each polynomial $f \in R_4$.

(c) It is given to you that $\ker(\varphi) = \langle f_1, f_2, f_3\rangle$ for some polynomials $f_1, f_2, f_3 \in R_4$. Find f_1, f_2, f_3. *Hint: part (e) may help.*

(d) Let h_1, h_2, h_3 be the 2 by 2 minors of the matrix $M = \begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \end{bmatrix}$. Consider the ideal $I = \langle h_1, h_2, h_3\rangle$. Show that I does not change if one applies elementary row operations to the matrix M.

(e) Take the ideal $J = \langle x_1x_4 - x_2x_3\rangle$ in R_4. Express J as kernel of some ring homomorphism. You know such a homomorphism exists by WSH 10. You do not need to prove that the proposed homomorphism has J as its kernel. Hopefully you will be able to prove this by the end of the semester.

(f) Prove that the ideal J is not a maximal ideal.

(a) Check the three condtions to be an ideal

- $0 = 0f_1 + \ldots + 0f_k \in \langle f_1, f_2, \ldots f_k\rangle$, where 0 is the polynomial zero.
- for any two combinations $g_1f_1 + g_2f_2 + \ldots + g_kf_k$ and $g'_1f_1 + g'_2f_2 + \ldots + g'_kf_k$ in $\langle f_1, f_2, \ldots f_k\rangle$, their sum $(g_1 + g'_1)f_1 + (g_2 + g'_2)f_2 + \ldots + (g_k + g'_k)f_k \in \langle f_1, f_2, \ldots f_k\rangle$
- for $g_1f_1 + g_2f_2 + \ldots + g_kf_k \in \langle f_1, f_2, \ldots f_k\rangle$ and $h \in R_n$, we have $h(g_1f_1 + g_2f_2 + \ldots + g_kf_k) = (hg_1)f_1 + (hg_2)f_2 + \ldots + (hg_k)f_k \in \langle f_1, f_2, \ldots f_k\rangle$.

(b) Note every polynomial in R_4 is of the form

$$a_{0000} + a_{1000}x_1 + a_{0100}x_2 + \ldots + a_{nmkl}x_1^n x_2^m x_3^k x_4^l, \text{ for some } n, m, k, l \in \mathbb{N} \cup \{0\}.$$

So, by the definition of a ring homomorphism

$$\begin{aligned} &\varphi(a_{0000} + a_{1000}x_1 + a_{0100}x_2 + \ldots + a_{nmkl}x_1^n x_2^m x_3^k x_4^l) \\ &= \varphi(a_{0000}) + \varphi(a_{1000})\varphi(x_1) + \varphi(a_{0100})\varphi(x_2) + \ldots + \varphi(a_{nmkl})\varphi(x_1)^n\varphi(x_2)^m\varphi(x_3)^k\varphi(x_4)^l = * \end{aligned}$$

From the last homework, a ring homomorphism map each rational number to itself. This, and the information on $\varphi(x_i)$ for $i = 1, 2, 3, 4$ conclude

$$\begin{aligned} * &= a_{0000} + a_{1000}\varphi(x_1) + a_{0100}\varphi(x_2) + \ldots + a_{nmkl}\varphi(x_1)^n\varphi(x_2)^m\varphi(x_3)^k\varphi(x_4)^l \\ &= a_{0000} + a_{1000}t_1^3 + a_{0100}t_1^2t_2 + \ldots + a_{nmkl}(t_1^3)^n(t_1^2t_2)^m(t_1t_2^2)^k(t_2^3)^l. \end{aligned}$$

So, the image of each polynomial in R_4 is completly determined. Note that you can generalize this observation to any ring homomorphism with R_n as domain.

(c) $ker(\varphi) = \langle x_1x_3 - x_3^2, x_2x_4 - x_3^2, x_1x_4 - x_2x_3\rangle$. Note that $\varphi(x_1x_3 - x_3^2) = \varphi(x_2x_4 - x_3^2) = \varphi(x_1x_4 - x_2x_3) = 0$.

Let $M = \begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \end{bmatrix}$. Then

$$I = (x_1x_3 - x_2^2,\ x_2x_4 - x_3^2,\ x_1x_4 - x_3x_2)$$

Let M' be the result of swapping the rows of M, and let I' be the ideal generated by the size 2 minors of M'.

Similarly, let M'' be the result of scaling a row (wolog, the first row of M) by a nonzero rational number q, and let I'' be the ideal generated by size 2 minors of M''.

Finally, let M''' be the result of replacing a row (wolog, the first row of M) by the sum of that row and a scalar multiple of the other row of M. Let I''' be the ideal generated by size 2 minors of M'''.

You are asked to show that

$$I = I' = I'' = I'''.$$

(d)

Lemma: Let R be a comm. ring, and suppose $I = (c_1, c_2, \dots, c_n)$. If $r \in R$ has a multiplicative inverse, then $I = (rc_1, rc_2, \dots, rc_n)$.

Proof: $(rc_1, \dots, rc_n) \subseteq I$

Let $x \in (rc_1, \dots, rc_n)$. Then by def, $\exists\, s_i \in R$ s.t. $x = s_1 rc_1 + \dots + s_n rc_n$. Since $c_i \in I$, this implies $x \in I$.

$I \subseteq (rc_1, \dots, rc_n)$

Let $x \in I$. Then by def, $\exists\, s_i \in R$ s.t. $x = s_1c_1 + \dots + s_nc_n$. Since r has a mult. inv.,

$$x = s_1 r^{-1} rc_1 + s_2 r^{-1} rc_2 + \dots + s_n r^{-1} rc_n.$$

Thus $x \in (rc_1, rc_2, \dots, rc_n)$.

$$M' = \begin{bmatrix} x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 \end{bmatrix}$$

Then $I' = (x_2^2 - x_1x_3,\ x_2x_3 - x_1x_4,\ x_3^2 - x_2x_4)$.

Since I' is generated by $-h_1, -h_2$ and $-h_3$ (where h_1, h_2, h_3 are the minors of M), $I' = I$.

Similarly, $M'' = \begin{bmatrix} qx_1 & qx_2 & qx_3 \\ x_2 & x_3 & x_4 \end{bmatrix}$, $q \neq 0$.

Then $I'' = (qx_1x_3 - qx_2^2,\ qx_2x_4 - qx_3^2,\ qx_1x_4 - qx_2x_3)$

$= (qh_1, qh_2, qh_3)$.

(Because $q \neq 0$, q has an inverse in $\mathbb{Q}$).

$$M''' = \begin{bmatrix} x_1 + qx_2 & x_2 + qx_3 & x_3 + qx_4 \\ x_2 & x_3 & x_4 \end{bmatrix}$$

$$I''' = \begin{pmatrix} (x_1 + qx_2)x_3 - (x_2 + qx_3)x_2, \\ (x_2 + qx_3)x_4 - (x_3 + qx_4)x_3, \\ (x_1 + qx_2)x_4 - (x_3 + qx_4)x_2 \end{pmatrix}$$

$= (h_1, h_2, h_3) = I$.

(e) J is the kernel of

$$\psi : R_4 \to \mathbb{Q}[t_1, t_2, t_3, t_4],\ \psi(x_1) = t_1t_3,\ \psi(x_2) = t_1t_4,\ \psi(x_1) = t_2t_3,\ \psi(x_1) = t_2t_4.$$

(f) $J \subset \langle x_1x_4 - x_2x_3, x_1 \rangle \neq R_4$.