R will denote a commutative ring with unity 1 throughout this problem set. Recall that the ideal generated by a set \( S \subseteq R \) is denoted \( \langle S \rangle \). We will often write \( \langle s_1, \ldots, s_n \rangle \) to mean \( \langle \{ s_1, \ldots, s_n \} \rangle \), e.g. \( \langle a \rangle \) instead of \( \langle \{ a \} \rangle \) for a principal ideal.

1. Let \( I \subseteq R \). We define the radical of \( I \) as the set
\[
\sqrt{I} := \{ a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N} \}.
\]
(a) Show that \( \sqrt{I} \subseteq R \) and \( I \subseteq \sqrt{I} \).

**Solution.** Let \( a, b \in I \) and \( r, s \in R \). So \( a^n \in I \) and \( b^m \in I \) for some \( n, m \in \mathbb{N} \). Now binomial expansion holds over any commutative ring and so
\[
(ra + sb)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} (ra)^{k}(sb)^{n+m-k-1}.
\]
(1.1)
Observe that
\[
k \leq n-1 \quad \text{iff} \quad m \leq n + m - k - 1
\]
and
\[
n \leq k \quad \text{iff} \quad n + m - k - 1 \leq m - 1.
\]
In other words, each summand in (1.1) always contain a factor \( a^n \) or \( b^m \). Hence
\[
(ra + sb)^{n+m-1} \in I
\]
and hence \( ra + sb \in \sqrt{I} \).

If \( a \in I \), then \( a^1 \in I \) and so \( a \in \sqrt{I} \).

(b) What are the radicals of the trivial ideals \( \langle 0 \rangle \) and \( \langle 1 \rangle \)?

**Solution.** By definition
\[
\sqrt{\langle 0 \rangle} = \{ a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N} \} = N(R),
\]
the nilradical of \( R \) defined in Problem Set 1, Problem 2. Clearly \( \sqrt{\langle 1 \rangle} = \sqrt{R} = R \).

(c) What is the radical of \( \sqrt{I} \)?

**Solution.** We claim that \( \sqrt{\sqrt{I}} = \sqrt{I} \). By (a), we have \( \sqrt{I} \subseteq \sqrt{\sqrt{I}} \). Let \( a \in \sqrt{\sqrt{I}} \).

Then there exists \( n \in \mathbb{N} \) such that \( a^n \in \sqrt{I} \); so there exists \( m \in \mathbb{N} \) such that \( (a^n)^m \in I \).

Since \( a^{nm} \in I \), we must have \( a \in \sqrt{I} \). Hence \( \sqrt{\sqrt{I}} \subseteq \sqrt{I} \).

(d) Suppose \( \sqrt{I} = R \), what is \( I \)?

**Solution.** Since \( 1 \in R = \sqrt{I} \), there exists \( n \in \mathbb{N} \) such that \( 1^n \in I \). So \( 1 \in I \) and so \( I = R \).

2. Let \( a \in R \) and \( m, n \in \mathbb{N} \). Show that
\[
\langle a^m - 1, a^n - 1 \rangle = \langle a^{\gcd(m,n)} - 1 \rangle.
\]

**Solution.** Let \( d = \gcd(m, n) \). Since \( d \mid n \), \( n = qd \) for some \( q \in \mathbb{N} \). So
\[
a^n - 1 = a^{qd} - 1 = (a^d - 1)(a^{q(d-1)} + a^{q(d-2)} + \cdots + x^q + 1).
\]

*Date: February 25, 2009 (Version 1.0).*
Hence \( a^n - 1 \in \langle a^d - 1 \rangle \). Likewise \( a^m - 1 \in \langle a^d - 1 \rangle \). Hence 
\[ \langle a^m - 1, a^n - 1 \rangle \subseteq \langle a^d - 1 \rangle. \]

Now for the reverse inclusion. Since \( d = \gcd(m, n) \), there exists \( a, b \in \mathbb{Z} \) such that 
\[ d = am + bn. \]

\( a \) and \( b \) must be of opposite signs as \( d \leq m, n \). Assume WLOG that \( a = -c \) where \( c \in \mathbb{N} \) and \( b \in \mathbb{N} \). Then 
\[ d = bn - cm. \]

Observe that 
\[ a^d - 1 = a^d - 1 - a^{d+cm} + a^{bn} \]
\[ = -a^d(a^{cm} - 1) + a^{bn} - 1 \]
\[ = -a^d(a^m - 1)(a^{c(m-1)} + \cdots + a^c + 1) + (a^n - 1)(a^{b(n-1)} + \cdots + a^b + 1) \]
and so \( a^d - 1 \) can be expressed in the form \( x(a^m - 1) + y(a^n - 1) \) where \( x, y \in R \). Hence 
\[ a^d - 1 \in \langle a^m - 1, a^n - 1 \rangle \] and thus 
\[ \langle a^d - 1 \rangle \subseteq \langle a^m - 1, a^n - 1 \rangle. \]

3. (a) Show that the ring \( \mathbb{Z}[(\sqrt{-2})] = \{ m+n\sqrt{-2} \mid m, n \in \mathbb{Z} \} \) is a Euclidean domain with valuation defined by \( \nu(m+n\sqrt{-2}) = m^2 + 2n^2 \). You need to (i) explain why it is an integral domain and (ii) prove that \( \nu \) is a valuation.

**SOLUTION.** It is clear that \( \mathbb{Z}[(\sqrt{-2})] \) is a subring of \( \mathbb{C} \) and therefore an integral domain. It remains to show that \( \nu \) defines a valuation. We will emulate the proof for Gaussian integers in the lectures. For nonzero \( a, b \in \mathbb{Z}[(\sqrt{-2})] \), write 
\[ \frac{a}{b} = r_1 + r_2\sqrt{-2} \]
where \( r_1, r_2 \in \mathbb{Q} \). We may find \( q_1, q_2 \in \mathbb{Z} \) such that 
\[ |q_1 - r_1| \leq \frac{1}{2} \quad \text{and} \quad |q_2 - r_2| \leq \frac{1}{2}. \]

Then 
\[ a = b(r_1 + r_2\sqrt{-2}) \]
\[ = b((q_1 + r_1 - q_1) + (q_2 + r_2 - q_2)\sqrt{-2}) \]
\[ = bq + r \]
where \( q = q_1 + q_2\sqrt{-2} \in \mathbb{Z}[(\sqrt{-2})] \) and 
\[ r = b(r_1 - q_1) + b(r_2 - q_2)\sqrt{-2} = a - bq \in \mathbb{Z}[(\sqrt{-2})]. \]

Furthermore, 
\[ \nu(r) = |b|^2 \times ((|r_1 - q_1|^2 + 2|r_2 - q_2|^2) \]
\[ \leq |b|^2 \times \left( \frac{1}{4} + 2 \times \frac{1}{4} \right) \]
\[ < \nu(b). \]

It is clear that \( \nu(a) \leq \nu(ab) \) since \( \nu(ab) = \nu(a)\nu(b) \) and \( \nu(b) \geq 1 \). Hence \( \nu \) is a valuation.

(b) Use (a) to find all integer solutions to the equation \( y^2 + 2 = x^3 \).

**SOLUTION.** By (a) and our discussion in the lectures, \( \mathbb{Z}[(\sqrt{-2})] \) is a unique factorization domain. Note that \( \mathbb{Z}[(\sqrt{-2})] = \{ -1, +1 \} \). Suppose \( (x_0, y_0) \in \mathbb{Z}^2 \) is a pair of integer solution to the equation. Then 
\[ x_0^3 = y_0^2 + 2 = (y_0 + \sqrt{-2})(y_0 - \sqrt{-2}). \]
So \( x_0 \mid (y_0 + \sqrt{-2})(y_0 - \sqrt{-2}) \) but \( x_0 \nmid y_0 + \sqrt{-2} \) and \( x_0 \nmid y_0 - \sqrt{-2} \) since the only integers that divide \( y_0 \pm \sqrt{-2} \) are \( \pm 1 \) and \( x_0 \) cannot be either of these (otherwise \( x_0^2 \leq 1 < y_0^2 + 2 \) yields a contradiction). Hence \( x_0 \) is not a prime element in \( \mathbb{Z}[\sqrt{-2}] \) and thus not irreducible. Let \( a = m + n\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}] \) be an irreducible divisor of \( x_0 \). Then there exists \( b \in \mathbb{Z}[\sqrt{-2}] \) such that

\[
ab = x_0.
\]

Since \( a \) divide \( x_0 \), it must also divide \( x_0^3 = (y_0 + \sqrt{-2})(y_0 - \sqrt{-2}) \). Since \( a \) is irreducible, we may assume WLOG that

\[
a \mid y_0 + \sqrt{-2}.
\]

Note that \( a \nmid y_0 - \sqrt{-2} \) (otherwise \( a \) must be \( \pm 1 \), contradicting \( a \) irreducible). But

\[
a^3b^3 = x_0^3 = (y_0 + \sqrt{-2})(y_0 - \sqrt{-2})
\]

and so

\[
a^3 \mid y_0 + \sqrt{-2}.
\]

Now observe that:

- if \( \bar{d} \in \mathbb{Z}[\sqrt{-2}] \), then \( \bar{d} \in \mathbb{Z}[\sqrt{-2}] \);
- if \( \bar{d} \) is irreducible in \( \mathbb{Z}[\sqrt{-2}] \), then \( \bar{d} \) is irreducible in \( \mathbb{Z}[\sqrt{-2}] \);
- if \( \bar{d} \mid e \) in \( \mathbb{Z}[\sqrt{-2}] \), then \( \bar{d} \mid \bar{e} \) in \( \mathbb{Z}[\sqrt{-2}] \).

Hence \( \bar{a} \) is irreducible in \( \mathbb{Z}[\sqrt{-2}] \) and

\[
a^3 \mid y_0 - \sqrt{-2}.
\]

Since \( \mathbb{Z}[\sqrt{-2}] \) is a Euclidean domain and therefore a unique factorization domain, by the equality of the factorizations

\[
a^3b^3 = \bar{a}^3\bar{b}^3,
\]

we get \( b = \bar{a} \). Hence

\[
y_0 + \sqrt{-2} = a^3 = (m + n\sqrt{-2})^3.
\]

In other words,

\[
\begin{align*}
y_0 &= m^3 - 6mn^2, \\
1 &= 3m^2n - 2n^3 = n(3m^2 - 2n^2),
\end{align*}
\]

from which we can see that the only solutions are

\[
\begin{align*}
y_0 &= 5, \\
x_0 &= 3, \quad \text{and} \quad \begin{cases} y_0 = -5, \\
x_0 = 3. \end{cases}
\end{align*}
\]

(c) Is the ring \( \mathbb{Z}[3i] = \{ m + 3ni \mid m, n \in \mathbb{Z} \} \) a Euclidean domain?

**SOLUTION.** \( \mathbb{Z}[3i] \) is an integral domain for the same reason as in (a). However it is not a Euclidean domain because it is not a unique factorization domain (recall from lectures that EDs are necessarily UFDs). To show the last assertion, note that 10 may be factorized in two different ways in \( \mathbb{Z}[3i] \),

\[
10 = 2 \cdot 5 = (1 + 3i)(1 - 3i).
\]

We want to show that 2 is irreducible in \( \mathbb{Z}[3i] \). Note that for any \( z = m + 3ni \in \mathbb{Z}[3i] \), \( |z|^2 = m^2 + 9n^2 \) is an integer. So if \( |z|^2 < 9 \), then \( n = 0 \) and \( z = m \). Let \( z, w \in \mathbb{Z}[3i] \) be such that

\[
2 = zw.
\]

Then

\[
4 = |2|^2 = |z|^2|w|^2
\]

and by our previous observation, we must have \( z = \pm 2 \) and \( w = \pm 1 \) or vice versa. Hence 2 is irreducible. If \( \mathbb{Z}[3i] \) were a unique factorization domain, then we must have either
2 \mid 1 + 3i \text{ or } 2 \mid 1 - 3i \text{ (since irreducibles are prime in a UFD) but this is a contradiction since } \frac{1 + 3i}{2} = \frac{1}{2} + \frac{3}{2}i \notin \mathbb{Z}[3i].

4. Consider the following subsets of \( \mathbb{R}[x] \),

\[ S_1 = \{ f(x) \in \mathbb{R}[x] \mid f(2) = f'(2) = f''(2) = 0 \}, \]
\[ S_2 = \{ f(x) \in \mathbb{R}[x] \mid f(1) = f(2) = f(3) = 0 \}, \]
\[ S_3 = \{ f(x) \in \mathbb{R}[x] \mid f(1) = f'(2) = f''(3) = 0 \}. \]

(a) Which of these are ideals of \( \mathbb{R}[x] \)? Prove your answers.

**Solution.** Note that a nonempty subset \( S \) of a ring is an ideal iff \( a_1s_1 + a_2s_2 \in S \) for all \( a_1, a_2 \in R \) and \( s_1, s_2 \in S \). Hence \( S_1 \) and \( S_2 \) are ideals while \( S_3 \) is not.

Let \( f_1(x), f_2(x) \in S_1 \) and \( a_1(x), a_2(x) \in \mathbb{R}[x] \). Let \( p(x) = a_1(x)f_1(x) + a_2(x)f_2(x) \). Then since \( f_i(2) = f'_i(2) = f''_i(2) = 0 \) for \( i = 1, 2 \), using the product rule for derivatives, we get

\[ p(2) = a_1(2)f_1(2) + a_2(2)f_2(2) = 0, \]
\[ p'(2) = a'_1(2)f_1(2) + a_1(2)f'_1(2) + a'_2(2)f_2(2) + a_2(2)f'_2(2) = 0, \]
\[ p''(2) = a''_1(2)f_1(2) + 2a'_1(2)f'_1(2) + a_1(2)f''_1(2) + a''_2(2)f_2(2) + 2a'_2(2)f'_2(2) + a_2(2)f''_2(2) = 0, \]

and so \( p(x) \in S_1 \).

Let \( f_1(x), f_2(x) \in S_2 \) and \( a_1(x), a_2(x) \in \mathbb{R}[x] \). Let \( p(x) = a_1(x)f_1(x) + a_2(x)f_2(x) \). Then since \( f_i(1) = f_i(2) = f_i(3) = 0 \) for \( i = 1, 2 \), we get

\[ p(1) = a_1(1)f_1(1) + a_2(1)f_2(1) = 0, \]
\[ p(2) = a_1(2)f_1(2) + a_2(2)f_2(2) = 0, \]
\[ p(3) = a_1(3)f_1(3) + a_2(3)f_2(3) = 0, \]

and so \( p(x) \in S_2 \).

Note that \( f(x) = x^3 - 9x^2 + 24 - 16 \) satisfies

\[ f(1) = f'(2) = f''(3) = 0 \]

and so \( f(x) \in S_3 \). Now take \( x \in \mathbb{R}[x] \) and observe that for \( p(x) = xf(x) \),

\[ p''(3) = -6 \neq 0. \]

Hence \( p(x) \notin S_3 \).

(b) For the ones that are ideals, which of them are principal?

**Solution.** We know from the lectures that \( \mathbb{R}[x] \) is a Euclidean domain with valuation \( \deg : \mathbb{R}[x] \setminus \{0\} \to \mathbb{N} \cup \{0\} \) and thus a principal ideal domain. Hence \( S_1 \) and \( S_2 \) are both principal.

(c) Find a generator for each principal ideal.

**Solution.** Again we know from the lectures that a generator of \( S_i \) must have minimal valuation among all (nonzero) elements of \( S_i, i = 1, 2 \).

Let \( f(x) \in S_1 \) be a generator. Note that by repeated division, we may express \( f(x) \) as

\[ f(x) = a_0 + a_1(x-2) + a_2(x-2)^2 + a_3(x-2)^3 + \cdots + a_d(x-2)^d \]

where \( d = \deg f(x) \). Now the condition \( f(2) = f'(2) = f''(2) = 0 \) implies that

\[ a_0 = f(2) = 0, \quad a_1 = f'(2) = 0, \quad a_2 = \frac{1}{2}f''(2) = 0, \]

and so

\[ f(x) = (x-2)^3[a_3 + a_4(x-2) + \cdots + a_d(x-2)^{d-3}]. \]
Since $f(x)$ must have minimal valuation, we must have $a_4 = \cdots = a_d = 0$ and $a_3 \neq 0$. Hence a generator of $S_1$ is given by $(x - 2)^3$.

Let $f(x) \in S_2$ be a generator. The condition $f(1) = f(2) = f(3) = 0$ implies that $x - 1, x - 2, x - 3$ must all divide $f(x)$ — a consequence of the Remainder Theorem. Hence the product $(x - 1)(x - 2)(x - 3)$ must divide $f(x)$ and so

$$f(x) = (x - 1)(x - 2)(x - 3)q(x).$$

Since $f(x)$ must have minimal degree, $q(x)$ must be a (non-zero) constant. Hence a generator of $S_2$ is given by $(x - 1)(x - 2)(x - 3)$.

5. Let $T$ be the ring of all real trigonometric polynomials

$$f(x) = a_0 + \sum_{n=1}^{d} a_n \cos nx + b_n \sin nx,$$

where $a_0, \ldots, a_d, b_1, \ldots, b_d \in \mathbb{R}$ and $d \in \mathbb{N} \cup \{0\}$. For any $f(x) \in T$, define $\deg(f(x)) = d$ where $a_d$ or $b_d \neq 0$.

(a) Show that $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

**Solution.** Let $f(x)$ and $g(x) \in T$ be given by

$$f(x) = a_0 + \sum_{n=1}^{N} a_n \cos nx + b_n \sin nx,$$

$$g(x) = c_0 + \sum_{m=1}^{M} c_m \cos mx + d_m \sin mx.$$

Using orthogonality of the set $\{1, \cos nx, \sin nx \mid n \in \mathbb{N}\}$, it is easy to see that

$$f(x) \equiv 0$$

iff all the coefficients of $f(x)$, i.e. $a_0, \ldots, a_d, b_1, \ldots, b_d$ are 0. Suppose $\deg f(x) = N$ and $\deg g(x) = M$. Since

$$(a_n \cos nx + b_n \sin nx)(c_m \cos mx + d_m \sin mx) =$$

$$\frac{a_n c_m - b_n d_m}{2} \cos(n + m)x + \frac{a_n d_m + b_n c_m}{2} \sin(n + m)x +$$

$$\frac{a_n c_m + b_n d_m}{2} \cos(n - m)x + \frac{a_n d_m - b_n c_m}{2} \sin(n - m)x,$$

we obtain

$$f(x)g(x) = \sum_{k=0}^{N+M} \left[ \left( \sum_{n+m=k} a_n c_m - b_n d_m \right) \cos kx + \left( \sum_{n+m=k} a_n d_m + b_n c_m \right) \sin kx \right].$$

The coefficients of $\cos(N + M)x$ and $\sin(N + M)x$ in $f(x)g(x)$ are

$$\frac{a_N c_M - b_N d_M}{2} \quad \text{and} \quad \frac{a_N d_M + b_N c_M}{2}$$

respectively. If both of them are 0, then

$$a_N c_M d_M = b_N d_M^2 = -b_N c_M^2$$
and so $b_N(c^2_M + d^2_M) = 0$. Since $c^2_M + d^2_M \neq 0$, $b_N = 0$. Then we have $a_N c_M = a_N d_M = 0$. Hence $a_N = 0$, which contradicts $a_N$ or $b_N \neq 0$. Thus we have proved that
\[ \deg(f(x)g(x)) = N + M = \deg f(x) + \deg g(x). \]

(b) Prove that $T$ is an integral domain.

**SOLUTION.** By the degree equation proved in (a), $f(x)g(x) = 0$ can happen only if either $f(x) = 0$ or $g(x) = 0$. Hence $T$ is an integral domain.

(c) Is $T$ a unique factorization domain?

**SOLUTION.** If $f(x)g(x) = 1$, then the degree equation implies that $\deg f(x) = 0 = \deg g(x)$. Hence the units are $T^* = \{-1, +1\}$. Obviously, in $T$ we have
\[
\cos 2x = (\cos x + \sin x)(\cos x - \sin x) = (1 + \sqrt{2}\sin x)(1 - \sqrt{2}\sin x).
\]

Again by the degree equation, all factors $\cos x \pm \sin x$ and $1 \pm \sqrt{2}\sin x$ are irreducible, and $\cos x \pm \sin x$ and $1 \pm \sqrt{2}\sin x$ are not associates. Thus $\cos 2x$ in $T$ does not have a unique factorization into irreducible elements. Hence $T$ is not a unique factorization domain.