Set $\phi = \frac{1}{2}(1 + \sqrt{5})$, the Golden Ratio, and $\overline{\phi} = \frac{1}{2}(1 - \sqrt{5})$. Set 

$$Z[\phi] = \{a + b\phi : a, b \in Z\}$$

For $\alpha = a + b\phi \in Z[\phi]$ set $\overline{\alpha} = a + b\overline{\phi}$.

1. Show that the map $\psi(\alpha) = \overline{\alpha}$ is a ring isomorphism from $Z[\phi]$ to itself. That is, show it is a ring homomorphism and a bijection from $Z[\phi]$ to itself. (Isomorphisms from an object to itself are called automorphisms, complex conjugation being the best known example. They play a central role in Galois Theory.)

**Solution:** As $\overline{\phi} = 1 - \phi$, $\psi$ maps $Z[\phi]$ to itself. As $\psi^2$ is the identity, it is a bijection. Clearly $\psi(0) = 0, \psi(1) = 1$. The hardest is that $\psi$ preserves multiplication, that

$$(a + b\phi)(c + d\phi) = a + b\phi c + d\phi$$

Here one can multiply out (there are some general Galois Theory principles at work), the key point that $\overline{\phi^2} = \overline{\phi}$.

2. Set $d(\alpha) = |\alpha\overline{\alpha}|$.

   (a) Show $d(a + b\phi) = |a^2 + ab - b^2|$.  

**Solution:** $(a + b\phi)(a + b\overline{\phi}) = a^2 + ab(\phi + \overline{\phi}) + b^2\phi\overline{\phi}$ and $\phi + \overline{\phi} = 1$ and $\phi\overline{\phi} = -1$.

   (b) Show $d(\alpha\beta) = d(\alpha)d(\beta)$ for all $\alpha, \beta \in Z[\phi]$.  

**Solution:** $|\alpha\beta\overline{\alpha}\overline{\beta}| = |\alpha\overline{\alpha}| \cdot |\beta\overline{\beta}|$

   (c) Show $\alpha$ is a unit in $Z[\phi]$ if $d(\alpha) = 1$.  

**Solution:** If $d(\alpha) = 1$, $\alpha\overline{\alpha} = \pm 1$ so $\alpha^{-1} = \pm\overline{\alpha} \in Z[\phi]$. Conversely if $\alpha$ is a unit there exists $\beta$ with $\alpha\beta = 1$ do $d(\alpha)d(\beta) = d(1) = 1$ so $d(\alpha) = 1$.

3. Now we describe the units of $Z[\phi]$.

   (a) Show $\phi$ is a unit.  

**Solution:** $\phi(-\overline{\phi}) = 1$
(b) Show there is no unit \( \alpha \) with \( 1 < \alpha < \phi \). (Idea: If so, \(|\alpha| < 1\) (why?) so \( \alpha - \overline{\alpha} = b\sqrt{5} \) would be “small” and \( \alpha + \overline{\alpha} = 2a + b \) would be “small.” The various cases \( a, b \) “small” are done ad hoc.
Solution: A unit implies \( d(\alpha) = \alpha\overline{\alpha} = \pm 1 \), so \(|\alpha| \cdot |\overline{\alpha}| = 1 \) and \(|\alpha| > 1 \) so \(|\alpha| < 1 \), that is, \( \alpha \in (-1, +1) \). We’re given \( \alpha \in (1, 6 \cdots) \).
Then \( b\sqrt{5} = \alpha - \overline{\alpha} \in (0, 2 \cdots) \). Thus \( b = 1 \). Also \( \alpha + \overline{\alpha} \in (0, 3 \cdots) \) and is \( 2a + 1 \) so we must have \( a = 0 \) or \( a = 1 \). Neither gives \( 1 < \alpha < \phi \) \((a = 0, b = 1 \text{ gives } \alpha = \phi) \) so \( \alpha \) doesn’t exist.

(c) Show that if \( \beta > 1 \) is a unit then \( \beta = \phi^n \) for some positive integer \( n \).
Solution: For some \( n \geq 0 \), \( \phi^n \leq \beta < \phi^{n+1} \). Set \( \gamma = \beta\phi^{-n} \). Then \( \gamma \) is a unit and \( 1 \leq \gamma < \phi \), a contradiction.

(d) Show that all units are of the form \( \pm \phi^n \) for some \( n \in \mathbb{Z} \).
Solution: Units in \((0, 1)\) are multiplicative inverses of units in \((1, \infty)\) and so will be \( \phi^n \) with \( n < 0 \). Negative units are negatives of positive units and so will be \(-\phi^n\).

4. Show that \( \mathbb{Z}[\phi] \) is a Euclidean Domain with size function \( d \). Illustrate your argument by setting \( a = 10 + 15\phi \), \( b = 5 + \phi \) and finding \( q, r \in \mathbb{Z}[\phi] \) with \( a = qb + r \) and \( r = 0 \) or \( d(r) < d(b) \)
Solution: We follow the argument for \( \mathbb{Z}[i] \). Let \( \alpha, \beta \in \mathbb{Z}[\phi] \). Write \( \gamma = \overline{\alpha} = x + y\phi \) with \( x, y \in \mathbb{Q} \). We invert by
\[
\frac{1}{a + b\phi} = \frac{\overline{a} + b\overline{\phi}}{a^2 + ab - b^2} = \frac{a + b(1 - \phi)}{a^2 + ab - b^2}
\]
Select \( x_0, y_0 \in \mathbb{Z} \) with \( |x - x_0| \leq \frac{1}{2}, |y - y_0| \leq \frac{1}{2} \). Set \( q = x_0 + y_0\phi \).
Then \( r = \alpha - q\beta = \beta[w + v\phi] \) with \( w, v \in \mathbb{Q}, |w|, |v| \leq \frac{1}{2} \). The function \( d(\cdot) \) is multiplicative on the field of all \( w + v\phi, w, v \in \mathbb{Q} \), so \( d(r) = d(\beta)|w^2 + vw - v^2| \). But with \( w, v \in [-\frac{1}{2}, +\frac{1}{2}], |w^2 + vw - v^2| \leq \frac{1}{2} \).
For the particular values \( a, b \),
\[
\frac{10 + 5\phi}{5 + \phi} = \frac{10 + 5\phi}{5 + \phi} = \frac{45 + 65\phi}{29}
\]
(Here we used \( \overline{\phi} = 1 - \phi \) and \( \phi^2 = 1 + \phi \).) so we take \( q = 2 + 2\phi \) and then \( r = a - bq = -2 + \phi \) and \( d(r) = 1 < d(b) = 29 \).

5. Show that an integer prime \( p \) is a prime in \( \mathbb{Z}[\phi] \) iff the Diophantine equation \( x^2 + xy + y^2 = \pm p \) has no solution. (Diophantine means that...
6. Here we show that every ideal $I \subset \mathbb{Z}[x]$ is generated by a finite number of elements. Fix an ideal $I \neq \{0\}$.

(a) Let $J$ be zero and the set of leading coefficients of the $0 \neq f(x) \in I$. Show $J$ is an ideal in $\mathbb{Z}$.

Solution: The only hard part is closure under addition. Say $a, b \in J$. Then there are $f(x) = ax^i + \cdots$ and $g(x) = bx^j + \cdots$. WLOG say $i \leq j$. Then $x^{j-i} f(x) + g(x) = (a+b)x^j + \cdots \in I$ so $a+b \in J$.

(b) With $J$ above, write $J = (c)$. Let $f(x) \in I$ have degree $n$ and lead coefficient $c$. Show that for any $g(x) \in I$ there exist $q(x), r(x) \in \mathbb{Z}[x]$ with $g(x) = f(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg(r(x)) < n$.

Solution: We must show that division “works.” Formally we use induction on the degree $m$ of $g(x)$. For $m < n$ simply set $q(x) = 0, r(x) = g(x)$. Now assume for all $m' < m$ and let $g(x) = dx^{m'} + \cdots$. Critically, $c|d$. Then $g(x) - (d/c)x^{m-n}f(x)$ is either zero or has degree $m' < m$. If its zero we are done. Else by induction we express

$$g(x) - (d/c)x^{m-n}f(x) = q_1(x)f(x) + r(x)$$

so that

$$g(x) = [q_1(x) + (d/c)x^{m-n}]f(x) + r(x)$$

(c) For each $0 \leq i < n$ let $J_i$ be the set of leading coefficients of polynomials of degree $i$. Show $J_i$ is an ideal in $\mathbb{Z}$.

Solution: Like $J$ above, but easier.

(d) With $J_i$ above, write $J_i = (c_i)$. Let $f_i(x) \in I$ have degree $i$ and lead coefficient $c_i$. Prove

$$I = (f_0(x), f_1(x), \ldots, f_{n-1}(x), f(x))$$

Solution: Let $g(x) \in I$. First (above) find $q_n(x), r_n(x)$ with
\[
g(x) = q_n(x)f(x) + r_n(x) \quad \text{and} \quad r_n(x) = 0 \quad (\text{in which case we are done}) \quad \text{or} \quad \deg(r_n(x)) < n.
\]
Informally, with \( \deg(r_n(x)) = i \), we now divide \( r_n(x) \) by \( f_i(x) \) and get a new remainder with degree strictly less than \( i \). Formally, we show by induction for \( 0 \leq i < n \) that if \( r_i(x) \in I \) of degree \( i \) then \( r_i(x) \in (f_0(x), \ldots, f_i(x)) \). For \( i = 0 \) all constants in \( I \) are multiples of the constant \( f_0(x) \). Assume for \( i' < i \). Let \( r_i(x) = d_i x^i + \cdots \) so \( c_i | d_i \). Then \( r_i(x) - (d_i/c_i) f_i(x) \) is either zero (so we’re done) or has degree \( i' < i \), in which case we’re done by induction.