1. An element \( u \in R \) is called a unit if it has a multiplicative inverse, that is, there exists an element \( v \in R \) such that \( uv = 1 \). (When this occurs we can write \( v = u^{-1} \) or \( v = \frac{1}{u} \).) Let \( U \) be the set of units of \( R \). Show that \( U \) forms a group under multiplication. The template for this is:

(a) Identity: \( 1 \in U \)

(b) Inverse: If \( u \in U \) then \( u^{-1} \in U \).

(c) Product: If \( u, v \in U \) then \( uv \in U \).

Solution:

(a) Identity: As \( 1 \cdot 1 = 1 \), \( 1 \in U \).

(b) Inverse: If \( u \in U \) then there is an element \( v = u^{-1} \in R \). As \( vu = 1 \), \( v \in U \).

(c) Product: If \( u, v \in U \) there exist \( w, x \in R \) with \( uw = vx = 1 \) but then \((uv)(wx) = 1\) so \( uv \in U \).

2. Define (this will be standard)

\[ Z[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \]

Show that \( Z[\sqrt{2}] \) is a Ring. The template for showing \( R \) is a ring when \( R \) is a subset of the complex numbers is:

(a) Identity: \( 0 \in R \)

(b) Inverse: If \( u \in R \) then \(-u \in R \).

(c) Sum: If \( u, v \in R \) then \( u + v \in R \).

(d) Product: If \( u, v \in R \) then \( uv \in R \).

Solution:

(a) Identity: \( 0 = 0 + 0\sqrt{2} \in Z[\sqrt{2}] \)

(b) Inverse: If \( u \in Z[\sqrt{2}] \) then \( u = a + b\sqrt{2} \) for some \( a, b \in \mathbb{Z} \) so \(-u = (-a) + (-b)\sqrt{2} \in Z[\sqrt{2}] \).

(c) Sum: If \( u, v \in Z[\sqrt{2}] \) then \( u = a + b\sqrt{2} \), \( v = c + d\sqrt{2} \) so \( u + v = (a + c) + (b + d)\sqrt{2} \in Z[\sqrt{2}] \).
(d) **Product:** If \( u, v \in \mathbb{Z}[\sqrt{2}] \) then \( u = a + b\sqrt{2}, \ v = c + d\sqrt{2} \) so
\[
\begin{aligned}
u v &= (ac + 2bd) + (ad + bc)\sqrt{2}
\end{aligned}
\]

3. Let \( \alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \). Show

(a) If \( a^2 - 2b^2 = \pm 1 \) then \( \alpha \) is a unit.

**Solution:** (Caution: Yes, the inverse of a nonzero element will exist as a real number, the problem here is to show that that inverse is in the ring.) We “rationalize the denominator”:
\[
\begin{aligned}
\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2 - 2b^2}
\end{aligned}
\]

With the denominator \( \pm 1 \), both \( a/(a^2 - 2b^2) \) and \( -b/(a^2 - 2b^2) \) are integers.

(b) (*) [The asterisk indicates a more difficult, but still required, problem.] If \( \alpha \) is a unit then \( a^2 - 2b^2 = \pm 1 \).

**Solution:** If \( \alpha \) is a unit then we must have the coefficients of \( \alpha^{-1} \) integral so that \( a^2 - 2b^2 | a \) and \( a^2 - 2b^2 | b \). Squaring, \( (a^2 - 2b^2)^2 | a^2 \) \( (a^2 - 2b^2)^2 | b^2 \) so \( (a^2 - 2b^2)^2 | (a^2 - 2b^2) \) so \( (a^2 - 2b^2) | 1 \) so it is \( \pm 1 \).

4. Define (this will be standard)
\[
Q(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}
\]
Prove that \( Q(\sqrt{2}) \) is a field. The template for showing \( R \) is a field when \( R \) is a subset of the complex numbers is that given for a ring above plus: If \( \alpha \in F \) and \( \alpha \neq 0 \) then \( \alpha^{-1} \in F \).

**Solution:** The ring properties are basically the same as for \( \mathbb{Z}[\sqrt{2}] \) above. For multiplicative inverse we again write
\[
\begin{aligned}
\frac{1}{a + b\sqrt{2}} &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}
\end{aligned}
\]

Now the coefficients \( \frac{a}{a^2 - 2b^2}, \frac{-b}{a^2 - 2b^2} \) are ratios of elements of \( Q \) and so are in \( Q \). The only problem would be if the denominator \( a^2 - 2b^2 = 0 \). If \( b \neq 0 \) that would imply \( (a/b)^2 = 2 \), contradicting the irrationality of \( \sqrt{2} \). If \( b = 0 \) then \( a = 0 \) and \( 0 + 0\sqrt{2} = 0 \), which is not supposed to have a multiplicative inverse.
5. Set
\[ \omega = e^{2\pi i/3} = \frac{-1 + i\sqrt{3}}{2} \]

and set
\[ Z[\omega] = \{a + b\omega : a, b \in Z\} \]

[We use the notation \( e^{i\theta} = \cos \theta + i\sin \theta \). Any nonzero complex \( \alpha \) may be uniquely written \( \alpha = re^{i\theta} \) with \( r > 0 \) real and \( 0 \leq \theta < 2\pi \) and has polar coordinates \( (r, \theta) \) when placed on the complex plane.]

(a) Draw a careful picture marking the points of \( Z[\omega] \) on the complex plane. You should get a pleasing pattern.

Solution: Click on graph for picture. (Had the X,Y coordinates been drawn to the same scale you would “see” a nice hexagonal packing of the plane. Also, the plane is divided into equilateral triangles, such as that bounded by 0,1,\( \omega + 1 \).)

(b) Show \( Z[\omega] \) is a ring. (Product is the hard part!)

Solution: Same as \( Z[\sqrt{2}] \) above except for Product. As \( \omega^2 = -1 - \omega \) we have
\[(a+b\omega)(c+d\omega) = ac+(bc+ad)\omega+bd(-1-\omega) = (ac-bd)+(bc+ad-bd)\omega \]

(c) (*) Find all units (with proof that you have all!) of \( Z[\omega] \).

Solution: The units are \( 1, 1 + \omega, \omega, -1, -1 - \omega, -\omega \). These are the points of a regular hexagon on the unit circle and can also be written (changing the order) as \( e^{2\pi ij/6}, \) \( 0 \leq j \leq 5 \). Seen this way they are all units as \( e^{2\pi i j/6}e^{2\pi i(6-j)/6} = e^{2\pi i} = 1 \). Showing these are the only units is harder.

Claim: Every nonzero element \( \alpha = a + b\omega \in Z[\omega] \) has \( |\alpha| \geq 1 \).

Proof: Some calculation gives
\[ |\alpha|^2 = a^2 + b^2 - ab \]

This is not negative (as it is the square of a norm) nor zero (as \( \alpha \neq 0 \)) and it is integral so it is at least one. As \( |\alpha|^2 \geq 1, |\alpha| \geq 1 \). That is, no nonzero elements of \( Z[\omega] \) lie inside the unit circle. Let \( \alpha \) be a unit. Then \( |\alpha| \geq 1 \) and \( |\alpha^{-1}| \geq 1 \). As \( |\alpha^{-1}| = |\alpha|^{-1} \) this can only occur when \( |\alpha| = 1 \). So the units of \( Z[\omega] \) must lie on the unit circle. If you drew a good picture you can “see” that there are precisely six such points but how to prove that. We have the equation
\[ |\alpha|^2 = a^2 + b^2 - ab = 1 \]
Hmmmm. Well, if \( a = 0 \) we have \( b^2 = 1 \), \( b = \pm 1 \), giving the units \( \pm \omega \). If \( b = 0 \) then \( a^2 = 1 \), \( a = \pm 1 \), giving the units \( \pm 1 \). Now suppose \( a, b \neq 0 \). If \( a, b \) have opposite signs we rewrite \( 1 = (a + b)^2 - 3ab \) but \( (a + b)^2 \geq 0 \) and \(-3ab \geq 3\) so no solutions there. Finally, suppose \( a, b \) have the same sign. We rewrite \( 1 = (a - b)^2 + ab \). Both terms are nonnegative and the second is strictly positive so we must have \( a - b = 0 \) and \( ab = 1 \) and there are two solutions \( a = b = 1 \) (the unit \( 1 + \omega \)) and \( a = b = -1 \) (the unit \( -1 - \omega \)).

Whew! That was pretty complicated. There are other more geometric approaches. In general, the determining the units of a ring is a complicated and interesting undertaking.

Another approach: To check if \( \alpha = a + b\omega \) is a unit we calculate \( \alpha^{-1} \) by rationalizing the denominator, by multiplying by the complex conjugate. Here \( \omega \) has complex conjugate \( \bar{\omega} = -1 - \omega \).

We have
\[
\frac{1}{a + b\omega} = \frac{1}{a + b\omega} \frac{a + b(-1 - \omega)}{a + b(-1 - \omega)} = \frac{a + b(-1 - \omega)}{a^2 + b^2 - ab}
\]
where the denominator is \( \alpha \bar{\alpha} = |\alpha|^2 \). If \( a^2 + b^2 - ab = 1 \) (it can’t be \(-1\) as it is the square of \( |\alpha| \)) then \( \alpha \) is a unit. Conversely, to be a unit we would have to have \( a^2 + b^2 - ab = 1 \) dividing both \( a - b \) and \(-b\), so both \( a, b \), so then \((a^2 + b^2 - ab)^2\) would divide all of \( a^2, b^2, ab \) and thus would divide \( a^2 + b^2 - ab \). We conclude that for \( \alpha \) to be a unit we must have \( a^2 + b^2 - ab = \pm 1 \). That is, \( a^2 + b^2 - ab = 1 \) is a necessary and sufficient condition for \( \alpha = a + b\omega \) to be a unit.

Yet another approach: Which points of \( \mathbb{Z}[\omega] \) lie on or inside the unit circle? Well, we are looking at \( i + j\omega \) which are vectors (thinking of \( \mathbb{C} \) as the plane) of the form

\[
j\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) + i(1, 0)
\]

So the \( y \)-value is a multiple of \( \sqrt{3}/2 \). If it is on or inside the unit circle this must be in \([-1, +1]\) and so we need only consider \( j = 0, 1, -1 \). For each fixed \( y \) value of this form the points on the horizontal line are spread out exactly one apart. For \( j = 0 \) they are the integers and \( i = -1, 0, 1 \) gives the complex (and real) numbers \(-1, 0, 1 \). For \( j = 1 \) the \( x \)-values are \(-\frac{1}{2} + i \) and to be in
or on the unit circle we must have this in $[-1, +1]$ and the only possibilities are $i = 0, 1$ giving the complex numbers $\omega$ and $\omega + 1$. Similarly for $j = -1$ the $x$-values are $\frac{1}{2} + i$ and to be in or on the unit circle we must have this in $[-1, +1]$ and the only possibilities are $i = 0, -1$ giving the complex numbers $-\omega$ and $-\omega - 1$. Other than 0, there are no points in the interior of the unit circle and these six points on the unit circle. Any nonzero $\alpha \in \mathbb{Z}\omega$ not on the unit circle would then be outside the unit circle (i.e., $|\alpha| > 1$) so its inverse (as a complex number) would be inside the unit circle and hence not in $\mathbb{Z}\omega$. Thus the only possibilities for units are the six points on the unit circle and they all work.