Algebra V63.0349
Assignment 5
Solutions

Set φ = 1/2(1 + √5), the Golden Ratio, and ϕ = 1/2(1 − √5). Set

\[ Z[φ] = \{a + bφ : a, b ∈ Z\} \]

For α = a + bφ ∈ Z[φ] set \( \overline{α} = a + b\overline{φ} \).

1. Show that the map \( ψ(α) = \overline{α} \) is a ring isomorphism from \( Z[φ] \) to itself. That is, show it is a ring homomorphism and a bijection from \( Z[φ] \) 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 \( φ = 1 − φ \), \( ψ \) maps \( Z[φ] \) to itself. As \( ψ^2 \) is the identity, it is a bijection. Clearly \( ψ(0) = 0, ψ(1) = 1 \). The hardest is that \( ψ \) preserves multiplication, that

\[ (a + bφ)(c + dφ) = a + bφc + dφ \]

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

2. Set \( d(α) = |α\overline{α}| \).

   (a) Show \( d(a + bφ) = |a^2 + ab − b^2| \).

Solution: \( (a + bφ)(a + b\overline{φ}) = a^2 + ab(φ + \overline{φ}) + b^2φ\overline{φ} \) and \( φ + \overline{φ} = 1 \) and \( φ\overline{φ} = −1 \).

   (b) Show \( d(αβ) = d(α)d(β) \) for all \( α, β ∈ Z[φ] \).

Solution: \( |αβ\overline{αβ}| = |α\overline{α}| \cdot |β\overline{β}| \)

   (c) Show \( α \) is a unit in \( Z[φ] \) iff \( d(α) = 1 \).

Solution: If \( d(α) = 1 \), \( α\overline{α} = ±1 \) so \( α^{-1} = ±\overline{α} ∈ Z[φ] \). Conversely if \( α \) is a unit there exists \( β \) with \( αβ = 1 \) do \( d(α)d(β) = d(1) = 1 \) so \( d(α) = 1 \).

3. Now we describe the units of \( Z[φ] \).

   (a)

   (b) Show \( φ \) is a unit.

Solution: \( ϕ(−\overline{φ}) = 1 \)
(c) Show there is no unit \( \alpha \) with \( 1 < \alpha < \phi \). (Idea: If so, \(|\bar{\alpha}| < 1 \) (why?) so \( \alpha - \bar{\alpha} = b\sqrt{5} \) would be “small” and \( \alpha + \bar{\alpha} = 2a + b \) would be “small.” The various cases \( a, b \) “small” are done \textit{ad hoc}. 

\textbf{Solution:} \( \alpha \) unit implies \( d(\alpha) = \alpha \bar{\alpha} = \pm 1 \), so \( |\alpha| \cdot |\bar{\alpha}| = 1 \) and \( |\alpha| > 1 \) so \(|\bar{\alpha}| < 1 \), that is, \( \bar{\alpha} \in (-1, +1) \). We’re given \( \alpha \in (1, 1.6 \cdots) \). Thus \( b\sqrt{5} = \alpha - \bar{\alpha} \in (0, 2.6 \cdots) \). Thus \( b = 1 \). Also \( \alpha + \bar{\alpha} \in (0, 3.6 \cdots) \) and is \( 2a + 1 \) so we must have \( a = 0 \) or \( a = 1 \). Neither gives \( 1 < \alpha < \phi \) (\( a = 0, b = 1 \) gives \( \alpha = \phi \)) so \( \alpha \) doesn’t exist.

(d) Show that if \( \beta > 1 \) is a unit then \( \beta = \phi^n \) for some positive integer \( n \).

\textbf{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.

(e) Show that all units are of the form \( \pm \phi^n \) for some \( n \in \mathbb{Z} \).

\textbf{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. \textbf{Just for Fun:} In India twenty-twenty is very popular. What is it?

(a) A card game 
(b) A dance 
(c) A form of cricket 
(d) A television show

\textbf{Solution:} Twenty twenty is a modern form of cricket. Unlike classic forms, which often takes days, twenty twenty is completed in a few hours.

5. \textbf{Just for Fun:} In China what character will you \textit{not} see on the web?

(a) Mickey Mouse 
(b) Winnie the Pooh 
(c) James Bond 
(d) Cinderella

\textbf{Solution:} Winnie the Pooh is banned from the web because it is used as a negative reference toward Xi Jinping. (The physical resemblance is remarkable!)
6. Show that \( Z[\phi] \) is a Euclidean Domain with size function \( d \). Illustrate your argument by setting \( a = 10+15\phi, b = 5+\phi \) and finding \( q, r \in Z[\phi] \) with \( a = qb + r \) and \( r = 0 \) or \( d(r) < d(b) \).

**Solution:** We follow the argument for \( Z[i] \). Let \( \alpha, \beta \in Z[\phi] \). Write \( \gamma = \frac{\alpha}{\beta} = x + y\phi \) with \( x, y \in Q \). We invert by

\[
\frac{1}{a+b\phi} = \frac{a+b\phi}{a^2+ab-b^2} = \frac{a+b(1-\phi)}{a^2+ab-b^2}
\]

Select \( x_0, y_0 \in Z \) 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 \( w, v \in Q, |w|, |v| \leq \frac{1}{2} \). The function \( d(\cdot) \) is multiplicative on the field of all \( w + v\phi, w, v \in Q, \) so \( d(r) = d(\beta)|w^2 + w\phi - v^2| \) But with \( w, v \in [-\frac{1}{2}, +\frac{1}{2}], |w^2 + w\phi - v^2| \leq \frac{1}{2} \).

For the particular values \( a, b, \)

\[
\frac{10 + 5\phi}{5 + \phi} = \frac{10 + 5\phi 5 + \bar{\phi}}{5 + \phi 5 + \bar{\phi}} = \frac{45 + 65\phi}{29}
\]

(Here we used \( \bar{\phi} = 1 - \phi \) and \( \phi^2 = 1 + \phi \)) so we take \( q = 2 + 2\phi \) and then \( r = a - bq = -2 + \phi \) and \( d(r) = 1 < d(b) = 29 \).

7. Let \( d \geq 2 \) be squarefree, \( d \equiv 2 \) or 3 mod 4, and set

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

*Assume* the Diophantine equation \( |x^2 - dy^2| = 1 \) has a nontrivial (that is, \( x = \pm 1, y = 0 \)) solution. (This is true, though not easy to prove!) Prove that there exists a \( \beta \in Z[\sqrt{d}] \) such that the units of \( Z[\sqrt{d}] \) are all of the form \( \pm \beta^n, n \in Z \). (Idea: Follow problem 3 above.)

**Solution:** For \( \alpha = a + b\sqrt{d} \in Z[\sqrt{d}] \) set \( \overline{\alpha} = a - b\sqrt{d} \). Take a solution to \( |x^2 - dy^2| = 1 \) with \( x, y > 0 \) and set \( \kappa = x + y\sqrt{d}, \kappa\overline{\kappa} = \pm 1, \kappa \) is a unit. Suppose \( \alpha = a + b\sqrt{d} \) is a unit and \( 1 < \alpha < \kappa \). As \( a\overline{\kappa} = \pm 1, |

If \( a \) were negative, \( b \) would be positive and then \( \overline{\alpha} = a - b\sqrt{d} \) would be less than \(-1 \). So we can assume \( a \) is positive. Now as \( a - b\sqrt{d} \leq 1 \) we must have \( b \) positive as well.

As \( 1 < \alpha < \kappa \) and \(-1 \leq \overline{\kappa} \leq 1, 2a = \alpha + \overline{\alpha} \leq 1 + \kappa \). As \( a \) must be positive integral there are only a finite number of possibilities for \( a \) (not all of them work) and for each \( a \) at most two possibilities for \( b \)
with $a^2 - db^2 = \pm 1$. That is, there are only a finite number (maybe zero!) of units $1 < \alpha < \kappa$. Any finite set has a least element so let $\alpha$ be the smallest unit with $\alpha > 1$.

Let $\gamma > 1$ be a unit. There will be some $n \geq 1$ with $\alpha^n \leq \gamma < \alpha^{n+1}$. But then $\gamma \alpha^{-n}$ is a unit and $1 \leq \gamma \alpha^{-n} < \alpha$. As $\alpha$ was the smallest unit bigger than one, $\gamma \alpha^{-n} = 1$ so $\gamma = \alpha^n$.

Let $0 < \gamma < 1$ be a unit. Then $\gamma^{-1} > 1$ is a unit and $\gamma^{-1} = \alpha^n$ so that $\gamma = \alpha^{-n}$.

Finally, let $\gamma < 0$ be a unit. Then $-\gamma$ is a unit so $-\gamma = \alpha^m$, $m \in \mathbb{Z}$, so that $\gamma = -\alpha^m$.

**Another Approach** The key point is that there is a smallest unit $\alpha = x + y\sqrt{d}$ with $\alpha > 1$. Here is another way of doing this. First we split into cases depending on the signs of $x, y$.

(a) $x = 0$: No unit
(b) $y = 0$: Then $x = \pm 1$, no unit $> 1$.
(c) $x, y < 0$ Then $\alpha < 0$. No
(d) $x > 0, y < 0$. Then $\alpha = x - y\sqrt{d} > 1$ (as both $x, -y$ positive) but then $\alpha \alpha > 1$. No.
(e) $x < 0, y > 0$. Then $\alpha = x - y\sqrt{d} < -1$ (as both $x, -y$ negative) but the $|\alpha| > 1$ so $|\alpha \alpha| > 1$. No

We are left with the case $x, y$ both positive.

Claim: The values $x + y\sqrt{d}, x, y > 0$, when placed in increasing order, give a countable list – a first, second, third, etc. (Note: This is not true for any countable set. Look at, say, the elements $10 - 2^{-n}$ for $n = 0, 1, 2, \ldots$ and 12.) Why is this? For any real $K$ there are only a finite number of $x, y$ with $x + y\sqrt{d} \leq K$ (certainly at most $K^2$) and so those can be listed – any finite set can be listed. Now we just do this for each $K$ and put them together and get a countable list.

Now consider units $\alpha > 1$. We are given that there is some $\kappa = x + y\sqrt{d}$ of this form. Look at all the $x + y\sqrt{d} \leq \kappa$ with $x, y > 0$. Some of them are units and some aren’t – just look at the units. There are only a finite number of them and therefore there is a smallest.