Math 460
Homework 3

Trevor Klar

October 2, 2018

1. Show that $\langle 2-i \rangle$ (that is, the ideal generated by $2-i$) is maximal in $\mathbb{Z}[i]$ by following these steps:

   a. Define a map $\phi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 2-i \rangle$ by $\phi(n) = n + \langle 2-i \rangle$. Show ϕ is a ring homomorphism.

   Proof

   - Since $\phi(1) = 1 + \langle 2-i \rangle$, then ϕ maps unity to unity.
   - Let $a, b \in \mathbb{Z}$. Then
   $$\phi(a+b) = (a+b) + \langle 2-i \rangle = \big(a + \langle 2-i \rangle\big) + \big(b + \langle 2-i \rangle\big) = \phi(a) + \phi(b).$$
   - Let $a, b \in \mathbb{Z}$. Then
   $$\phi(ab) = (ab) + \langle 2-i \rangle = \big(a + \langle 2-i \rangle\big)\big(b + \langle 2-i \rangle\big) = \phi(a)\phi(b).$$

   Thus ϕ is a ring homomorphism. ■

   b. Now show ϕ is onto.

   Proof Let $(a+bi) + \langle 2-i \rangle \in \mathbb{Z}[i]/\langle 2-i \rangle$ be given. Choose $n = a + 2b$. This means that
   $$\phi(n) = \phi(a+2b) = (a+2b) + \langle 2-i \rangle = (a+bi) + \langle 2-i \rangle.$$
   To see that this last equality holds, observe that
   $$(a+2b) - (a+bi) = 2b - bi = b(2-i) \in \langle 2-i \rangle.$$
   Therefore we can produce an integer which ϕ maps to any element of $\mathbb{Z}[i]/\langle 2-i \rangle$, so ϕ is onto. ■

   c. Show $\ker\phi = 5\mathbb{Z}$.

   Proof ($\ker\phi \supseteq 5\mathbb{Z}$) Observe that $2 + \langle 2-i \rangle = i + \langle 2-i \rangle$. Then for all $5n \in 5\mathbb{Z}$,
   $$\begin{aligned} \phi(5n) &= 5n + \langle 2-i \rangle \\ &= (2^2+1)n + \langle 2-i \rangle \\ &= (i^2+1)n + \langle 2-i \rangle \\ &= \langle 2-i \rangle \end{aligned}$$
   Thus, $5\mathbb{Z} \subseteq \ker\phi$. ■

   Proof ($\ker\phi \subseteq 5\mathbb{Z}$) Let $k \in \ker\phi$ be given. Then $k \in \langle 2-i \rangle$, so there exists $a, b \in \mathbb{Z}$ such that
   $$k = (a+bi)(2-i) = (2a+b) + (-a+2b)i,$$
   which implies that $a = 2b$, and $k = 2a + b$. Thus
   $$\begin{aligned} k &= 2a + b \\ &= 2(2b) + b \\ &= 5b. \end{aligned}$$
   Therefore, for all $k \in \ker\phi$, we can find $b \in \mathbb{Z}$ such that $k = 5b$, so $\ker\phi \subseteq 5\mathbb{Z}$. ■

d. Now, use the FHT.
Therefore, since $\phi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 2-i \rangle$ is onto and $\ker \phi = 5\mathbb{Z}$, then

$$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 \cong \mathbb{Z}[i]/\langle 2-i \rangle$$

by the FHT. Since $\mathbb{Z}_5$ is a field, then so is $\mathbb{Z}[i]/\langle 2-i \rangle$, which means that $\langle 2-i \rangle$ is a maximal ideal in $\mathbb{Z}[i]$. ■

2. Show that $\langle 3-i \rangle$ (that is, the ideal generated by $3-i$) is not prime in $\mathbb{Z}[i]$ by following these steps:

a. Define $\phi : \mathbb{Z} \to \mathbb{Z}[i]/\langle 3-i \rangle$ by $\phi(n) = n + \langle 3-i \rangle$. Show ϕ is an onto ring homomorphism.

Proof

- Since $\phi(1) = 1 + \langle 3-i \rangle$, then ϕ maps unity to unity.
- Let $a, b \in \mathbb{Z}$. Then

$$\phi(a+b) = (a+b) + \langle 3-i \rangle = \big(a + \langle 3-i \rangle\big) + \big(b + \langle 3-i \rangle\big) = \phi(a) + \phi(b).$$

- Let $a, b \in \mathbb{Z}$. Then

$$\phi(ab) = (ab) + \langle 3-i \rangle = \big(a + \langle 3-i \rangle\big)\big(b + \langle 3-i \rangle\big) = \phi(a)\phi(b).$$

- Let $(a+bi) + \langle 3-i \rangle \in \mathbb{Z}[i]/\langle 3-i \rangle$ be given. Choose $n = a + 3b$. Then since

$$(a+3b) - (a+bi) = b(3-i) \in \langle 3-i \rangle,$$

then

$$\phi(n) = (a+3b) + \langle 3-i \rangle = (a+bi) + \langle 3-i \rangle.$$

Therefore, ϕ is an onto homomorphism. ■

b. Show $\ker \phi = 10\mathbb{Z}$.

Proof **($\ker \phi \supseteq 10\mathbb{Z}$)** Let $10n \in 10\mathbb{Z}$ be given. Observe that $3 + \langle 3-i \rangle = i + \langle 3-i \rangle$. Then

$$\begin{aligned} \phi(10n) &= 10n + \langle 3-i \rangle \\ &= (3^2+1)n + \langle 3-i \rangle \\ &= (i^2+1)n + \langle 3-i \rangle \\ &= \langle 3-i \rangle \end{aligned}$$

Thus $10\mathbb{Z} \subseteq \ker \phi$. ■

Proof **($\ker \phi \subseteq 10\mathbb{Z}$)** Let $k \in \ker \phi$ be given. Then $k \in \langle 3-i \rangle$, which means that there exists $a, b \in \mathbb{Z}$ such that

$$k = (a+bi)(3-i) = (3a+b) + (3b-a)i,$$

which means that $a = 3b$ and $k = 3a + b$. Thus

$$\begin{aligned} k &= 3a + b \\ &= 3(3b) + b \\ &= 10b \end{aligned}$$

Therefore, $\ker \phi \subseteq 10\mathbb{Z}$. ■

c. By FHT,

$$\mathbb{Z}/10\mathbb{Z} = \mathbb{Z}_{10} \cong \mathbb{Z}[i]/\langle 3-i \rangle,$$

so $\langle 3-i \rangle$ is not prime.

Proof If $\langle 3-i \rangle$ were prime, then $\mathbb{Z}[i]/\langle 3-i \rangle$ would be an integral domain. However, $\mathbb{Z}_{10}$ has zero divisors ($2 \times 5 = 0$), so neither ring is an integral domain, so $\langle 3-i \rangle$ is not prime. ■

3. Define $N : \mathbb{Z}[\sqrt{6}] \to \mathbb{Z}$ by $N\big(a + b\sqrt{6}\big) = a^2 - 6b^2$.

   a. Show that N is multiplicative, i.e. $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\sqrt{6}]$.

   Proof Let $x, y \in \mathbb{Z}[\sqrt{6}]$ be given. Then we can write $x = a + b\sqrt{6}$ and $y = c + d\sqrt{6}$. Then

$$\begin{aligned} N(xy) &= N\big((a + b\sqrt{6})(c + d\sqrt{6})\big) \\ &= N\big((ac + 6bd) + (ad + bc)\sqrt{6}\big) \\ &= a^2c^2 + 12abcd + 36b^2d^2 - 6a^2d^2 - 12abcd - 6b^2c^2 \\ &= a^2c^2 - 6a^2d^2 - 6b^2c^2 + 36b^2d^2 \\ &= (a^2 - 6b^2)(c^2 - 6d^2) \\ &= N(a + b\sqrt{6})N(c + d\sqrt{6}) \\ &= N(x)N(y) \end{aligned}$$

   and we are done. ■

   b. Use N to explain why the only invertible elements in $\mathbb{Z}[\sqrt{6}]$ have N of 1.

   Proof ($\implies$) Let $x \in \mathbb{Z}[\sqrt{6}]$ be invertible. Then there exists $y \in \mathbb{Z}[\sqrt{6}]$ such that $xy = 1$. Taking N of both sides, we find that

$$N(x)N(y) = N(xy) = N(1) = 1.$$

   Since $N(x), N(y) \in \mathbb{Z}$, then $N(x) = N(y) = \pm 1$. This means that if $x = a + b\sqrt{6}$, then

$$a^2 - 6b^2 = \pm 1.$$

   This second-order Diophantine equation has no solutions for the negative case, but infinitely many for the positive, i.e. $N(1) = N(-1) = N(5 + 2\sqrt{6}) = N(5 - 2\sqrt{6}) = 1$. Thus, any invertible element $x \in \mathbb{Z}[\sqrt{6}]$ is such that $N(x) = 1$. ■

   Proof ($\impliedby$) Let $x \in \mathbb{Z}[\sqrt{6}]$ with $N(x) = 1$. Then if we write $x = (a + b\sqrt{6})$, choose $y = (a - b\sqrt{6})$. Then

$$xy = (a + b\sqrt{6})(a - b\sqrt{6}) = a^2 - 6b^2 = N(x) = 1,$$

   so $xy = 1$ and x is invertible. ■

   c. Show that $\sqrt{6}$ is not an irreducible element in $\mathbb{Z}[\sqrt{6}]$ by writing it as a product of two non-invertible elements in $\mathbb{Z}[\sqrt{6}]$.

   Proof Since $N(\sqrt{6}) = -6$, we have that $\sqrt{6}$ is nonzero and not a unit. However,

$$(2 + \sqrt{6})(3 - \sqrt{6}) = \sqrt{6},$$

   so $\sqrt{6}$ is reducible. To confirm this, we check that $(2+\sqrt{6})$ and $(3-\sqrt{6})$ are non-units. $N(2+\sqrt{6}) = -2$ and $N(3 - \sqrt{6}) = 3$, and we know that $N(x) = 1$ for all $x \in U\big(\mathbb{Z}[\sqrt{6}]\big)$, so we are done. ■

   d. Prove that $(1 + \sqrt{6})$ is irreducible in $\mathbb{Z}[\sqrt{6}]$.

   Proof Suppose $x, y \in \mathbb{Z}[\sqrt{6}]$ such that $xy = (1 + \sqrt{6})$. Then

$$N(x)N(y) = N(1 + \sqrt{6}) = -5.$$

   Since $N(x), N(y) \in \mathbb{Z}$, Then $N(x), N(y)$ are 1,-5 or -1,5. We know already that there are no elements of $\mathbb{Z}[\sqrt{6}]$ with N of -1, so that means that either $N(x) = 1$ or $N(y) = 1$, and thus one of them is a unit. ■

   e. Prove that $(1 + \sqrt{6})$ is prime in $\mathbb{Z}[\sqrt{6}]$.

   Proof Suppose $(1 + \sqrt{6}) = ab$ for some $a, b \in \mathbb{Z}[\sqrt{6}]$. Since $(1 + \sqrt{6})$ is irreducible, then either a or b is a unit. If a is invertible, then $a^{-1}(1 + \sqrt{6}) = a^{-1}ab = b$, so $(1 + \sqrt{6})|b$. Otherwise if b is invertible, then $(1 + \sqrt{6})b^{-1} = abb^{-1} = a$, so $(1 + \sqrt{6})|a$. ■

4. Show that the domains $\mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{-7}]$ are not UFDs. Just look at how we did $\mathbb{Z}[\sqrt{-3}]$ in class.
Lemma The only units of $\mathbb{Z}[\sqrt{-n}]$ where $1 < n \in \mathbb{Z}$ are ± 1.

PROOF Consider $\eta : \mathbb{Z}[\sqrt{-n}] \to \mathbb{N}$ defined by $\eta(a+b\sqrt{-n}) = a^2+nb^2$. η is multiplicative for the same reasons as in (3a), so for any units x, y we have that $\eta(x)\eta(y) = \eta(1) = 1$. If we write $x = (a+b\sqrt{-n})$, then

$$\eta(x) = a^2 + nb^2 = 1,$$

which can only hold for $b = 0$, $a = \pm 1$ (since $a, b \in \mathbb{Z}$). ■

Now we prove that $\mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{-7}]$ are not UFDs.

a. **Claim.** $\mathbb{Z}[\sqrt{-6}]$ is not a UFD, because $(2+\sqrt{-6})(2-\sqrt{-6}) = 10 = (5)(2)$ and all of $2, 5, (2\pm\sqrt{-6})$ are irreducible.

PROOF To see that $(2+\sqrt{-6})$ is irreducible, observe that $(2+\sqrt{-6}) \neq \pm 1$ and thus is not a unit and nonzero. Suppose $xy = (2+\sqrt{-6})$ where $x, y \in \mathbb{Z}[\sqrt{-6}]$ are not units. Then $\eta(x)\eta(y) = \eta(2+\sqrt{-6}) = 10$, so

$$\eta(x) = (a^2 + 6b^2) = 5, 2.$$

This has no solutions, since $(a^2 + 6b^2) > 5$ for $b \neq 0$ and $5, 2$ are not square numbers. By the same argument, $(2-\sqrt{-6})$ is irreducible as well.
A similar argument shows that 5 is irreducible. Observe that $5 \neq \pm 1$ and thus is not a unit and nonzero. Suppose $xy =$ where $x, y \in \mathbb{Z}[\sqrt{-6}]$ are not units. Since $\eta(5) = \eta(5+6\sqrt{-6}) = 25$, then

$$\eta(x) = (a^2 + 6b^2) = 5,$$

and we have already seen that this has no solutions. The same argument shows that 2 is also irreducible. ■

b. **Claim.** $\mathbb{Z}[\sqrt{-7}]$ is not a UFD, because $(1+\sqrt{-7})(1-\sqrt{-7}) = 8 = 2^3$ and all of $2, (1\pm\sqrt{-7})$ are irreducible.

PROOF We use a similar proof as in (4a), and omit some notation. To see that $(1+\sqrt{-7})$ is irreducible, observe that $(1+\sqrt{-7}) \neq \pm 1$ and $\eta(x)\eta(y) = 8$, so

$$\eta(x) = (a^2 + 7b^2) = 2, 4.$$

Though $(2+0\sqrt{-7})$ is a solution to $\eta(x) = 4$, there are no solutions to $\eta(x) = 2$, so there is no such $x \in \mathbb{Z}[\sqrt{-7}]$ such that $2x = (1+\sqrt{-7})$. Thus we conclude that $(1+\sqrt{-7})$ is irreducible, and so is $(1-\sqrt{-7})$, since it has the same η. Also 2 is irreducible by the same reasoning as in the previous problem. ■