Homework 5 (Due Feb 26, 2025)

Jack Hyatt

MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Let R be a PID and let $a, b \in R$ not zero and not units. Assume $d = \gcd(a, b)$. Recall this implies that there exist elements $a', b' \in R$ s.t. $a = da'$ and $b = db'$.

   (a) Prove that $\gcd(a', b') = 1$.

   Proof. Let d' be a common divisor of a' and b'. Then $a' = d'a''$ and $b' = d'b''$. Then we have $a = dd'a''$ and $b = dd'b''$. So then dd'' is a common divisor of a and b. But d is already the greatest common divisor, making d' a unit.
   So since the only common divisors of a' and b' are units, then $\gcd(a', b') = 1$. ■

   (b) Let $\ell = a'b'd$ (note that his is equal to $(ab)/d$). Prove that ℓ is the least common multiple of a, b (meaning that $a|\ell, b|\ell$, and for any element $L \in R$, if $a|L$ and $b|L$ then $\ell|L$).

   Proof. With $a = da'$ and $b = db'$, we easily get $\ell = ab'$ and $\ell = ba'$. So $a|\ell$ and $b|\ell$.
   Let $L \in R$ with $a|L$ and $b|L$. So $L = an$ and $L = bm$ for some $n, m \in R$.

$$
\begin{aligned}
L =& an = da'n \\
L =& bm = db'm \\
\implies & a'n = b'm
\end{aligned}
$$

   Since $\gcd(a', b') = 1$, there exists $x, y \in R$ s.t. $a'x + b'y = 1$.

$$
\begin{aligned}
a'x + b'y &= 1 \\
n(a'x + b'y) &= n \\
a'nx + b'ny &= n \\
b'mx + b'ny &= n \\
b'(mx + ny) &= n
\end{aligned}
$$

   So then $b'|n$, and it is a similar argument for $a'|m$. So we have $n = b'z$ for some $z \in R$, meaning $L = da'n = da'b'z = \ell z$. So finally we have $\ell|L$. ■

2. (a) Prove that 5 is not irreducible as an element of $\mathbb{Z}[i]$.

We know that 5 is not irreducible because we can write $5 = (2-i)\cdot(2+i)$, and it is easy to see that the multiplicative inverse of $2-i$ would need to be $2/5+i/5 \notin \mathbb{Z}[i]$, and similarly for $2+i$. So neither $2-i$ or $2+i$ are units.

(b) If p is a prime number (i.e. prime as an element of $\mathbb{Z}$) and $p \equiv 3 \mod 4$, prove that p is irreducible as an element of $\mathbb{Z}[i]$.

Proof. BWOC, assume $p = fg$ with $f, g \in \mathbb{Z}[i]$ not units. Take $N(a+bi) = a^2 + b^2$ to be the usual norm for $\mathbb{Z}[i]$. We can take the norm of both sides of $p = fg$ to get

$$\begin{aligned} N(p) &= N(f)N(g) \\ p^2 &= N(f)N(g) \end{aligned}$$

Since $N(f)$ and $N(g)$ are both positive integers, they must be factors of p^2. Since p is prime, the possible factorizations of p^2 are limited to $p \cdot p$ or $1 \cdot p^2$. We can ignore the $1 \cdot p^2$ case since that would mean one of the factors, f or g, is a unit, but we assumed that was not the case.

So assume $N(f) = p$ and $N(g) = p$.

Then $f = a + bi$ for some $a, b \in \mathbb{Z}$, so $N(f) = a^2 + b^2 = p$. Since $0^2 \equiv 2^2 \equiv 0 \mod 4$ and $1^2 \equiv 3^2 \equiv 1 \mod 4$, we know that $a^2 \mod 4$ and $b^2 \mod 4$ must also be either 0 or 1. But then $a^2 + b^2 \not\equiv 3 \mod 4$, which is a contradiction since $p \equiv 3 \mod 4$.

■

3. Find $\gcd(5, 3-i)$ as elements in $\mathbb{Z}[i]$. Prove your answer.

Proof. Let the norm of $\mathbb{Z}[i]$ be the usual $N(a+bi) = a^2 + b^2$. Let $d = \gcd(5, 3-i)$.

Since d divides 5, its norm $N(d)$ must divide $N(5)$, which is $N(5) = 25$. Similarly, since d also divides $3-i$, $N(d)$ must also divide $N(3-i) = 10$.

Thus, $N(d)$ must be a common divisor of 25 and 10, giving $\gcd(25, 10) = 5$.

Since norms in $\mathbb{Z}[i]$ must be sums of squares, the possible values for $N(d)$ are either 1 or 5.

If $N(d) = 1$, then d is a unit. So let us assume this is not the case.

Then $N(d) = 5$, we solve for integers a, b such that $a^2 + b^2 = 5$.

The integer solutions are:

$$(\pm 2, \pm 1) \quad \text{or} \quad (\pm 1, \pm 2).$$

Thus, possible values for d are:

$$\pm(2+i), \quad \pm(2-i), \quad \pm(1+2i), \quad \pm(1-2i).$$

We will need to only check if $2+i$ and $2-i$ divides both 5 and $3-i$, as the pairs $2+i$ and $1-2i$, and $2-i$ and $1+2i$ are associates (the unit to multiply with is i).

$$(2 - i)(7/5 + i/5) = 3 - i$$

So then we know that $2 - i$ is not a divisor of $3 - i$ in $\mathbb{Z}[i]$, meaning it isn't a common divisor either.

$$(2 + i)(1 - i) = 3 - i \qquad (2 + i)(2 - i) = 5$$

Since $2 + i$ is a common divisor and has norm 5, which is the largest possible for a non-unit common divisor, we conclude $\gcd(5, 3 - i) = 2 + i$ (and its associates). ∎

4. Recall that $\mathbb{Z}[i]$ is a PID. Consider the ideal $I = (1 + 2i, 1 + 5i)$. Find a generator for I. Prove your answer.

   Proof. Finding the generator for I is only a matter of finding $\gcd(1 + 2i, 1 + 5i)$.

   Let the norm of $\mathbb{Z}[i]$ be the usual $N(a + bi) = a^2 + b^2$. Let $d = \gcd(1 + 2i, 1 + 5i)$.

   Since d divides $1 + 2i$, its norm $N(d)$ must divide $N(1 + 2i) = 5$. Similarly, since d also divides $1 + 5i$, $N(d)$ must also divide $N(1 + 5i) = 26$.

   Thus, $N(d)$ must be a common divisor of 5 and 26, giving 1 as the only possibility. So then d is a unit, which means $\gcd(1 + 2i, 1 + 5i) = 1$.

   So then $I = (1)$, which is the whole ring $\mathbb{Z}[i]$. ∎