MAT 1100 Homework 4

Michael Yu

1. 1. Suppose for contradiction I is principal. Then there is some $a \in \mathbb{Z}[x]$ such that $Ra = I$. Because $3 \in I$ we must have some $p \in R$ satisfying $pa = 3$, so a must be a degree 0 polynomial, *i.e.* just a constant term dividing 3. For the other element $s \coloneqq x^3 - x^2 + 2x - 1$ in I, there has to be a $q \in R$ satisfying $qa = s$, meaning that the constant term of q times a equals the unit constant term -1, implying a must be a unit, showing I is actually all of $\mathbb{Z}[x]$, which is a contradiction because $2 \notin I$ (2 is not in I because $3 \nmid 2$ and using any multiple of the second generator will cause the resulting polynomial to have degree more than 0).

2. $\mathbb{Z}[x]/I$ is not an integral domain because I is not prime. The product $(3x-3)(x^2+2) = 3x^3 - 3x^2 + 6x - 6 = 3(x^3 - x^2 + 2x - 1) - 1(3) \in I$ witnesses I not being prime, for the factors $3x - 3$ and $x^2 + 2$ are not in I for a similar reason as to why $2 \notin I$, explained above.

2. $\implies$ Since R is a PID, there is some $c \in R$ such that $\langle a, b\rangle = Rc$. I claim that $c = \gcd(a, b)$, from which the desired result follows. We use a lemma.
Lemma. $x \mid y \iff Rx \ni y \iff Rx \supset Ry$

Proof. [$\implies$] If $ax = y$ then $y \in Rx$ and $Ry \subseteq Rx$.

[$\impliedby$] If $Ry \in Rx$ then $y = 1y = rx$ for some $r \in R$ and so $y \in Rx$ and $x \mid y$. □

First we have that $a, b \in Rc$, *i.e.* $Ra, Rb \subseteq Rc$, so $c \mid a$ and $c \mid b$ by the lemma. Now if $q \mid a$ and $q \mid b$, then $Rq \ni a, b$, whence Rq, being an ideal, contains the smallest ideal containing a, b, *i.e.* the ideal $\langle a, b\rangle = Rc$, and so $q \mid c$. Thus we have shown $c = \gcd(a, b)$.

$\impliedby$ First I prove some general facts of UFDs.
Lemma. *Let R be a UFD and let $a, b \in R$.*

i. $\langle a, b\rangle \subseteq \langle \gcd(a, b)\rangle$

ii. Any ascending chain of principal ideals $\langle a_0\rangle \subseteq \langle a_1\rangle \subseteq \dots$ eventually stabilizes.

Proof.

i. Let $c \coloneqq \gcd(a, b)$, say with $h, f \in R$ satisfying $ch = a$ and $cf = b$. Then $ra + sb = rhc + sfc = (rh + sf)c \in Rc$, so $\langle a, b\rangle \subseteq \langle c\rangle$.

ii. $\langle a_n\rangle \subseteq \langle a_{n+1}\rangle$ means for some $r \in R$ that

$$a_n = ra_{n+1}$$

If $\langle a_n\rangle \neq \langle a_{n+1}\rangle$, then $a_{n+1} \notin \langle a_n\rangle$, and we know r must not be a unit, so by considering unique factorization into primes of the quantities in the equation above, we get that the number of prime factors of a_n strictly exceeds that of a_{n+1} (it does not matter if $a_n = 0$). Hence the chain stabilizes eventually.

□

Now I prove the desired result via the following program (assume now that $\gcd(a,b) \in \langle a,b\rangle$):

I. $\langle a,b\rangle = \langle \gcd(a,b)\rangle$

II. Every finitely generated ideal of R is principal.

III. Every ideal is finitely generated

The proofs follows:

I. Immediate by lemma(i.) and the problem assumption.

II. Immediate by induction using (I.).

III. Let I be an ideal. Well-order I in a sequence $\{a_\eta\}_{\eta\in\alpha}$ for some ordinal α. Recursively construct the subsequence $\{a_{\eta_\iota}\}_{\iota\in\beta}$ for some $\beta < \alpha$ satisfying $a_\delta \notin \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in\delta}$ for each $\gamma \in \beta$, in other words filter $\{a_\eta\}_{\eta\in\alpha}$ to get the subsequence $\{a_{\eta_\iota}\}_{\iota\in\beta}$ in which each successive element is not in the ideal generated by all the previous elements. It is easy to see by transfinite induction that the ideal generated by this subsequence is the same as that generated by the original sequence.

We have the strictly ascending subchain (restricting the sequence to those with index in ω)

$$\begin{array}{ccccccccc} \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in 0} & \subset & \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in 1} & \subset & \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in 2} & \subset & \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in 3} & \subset & \dots \\ \langle\,\rangle & \subset & \langle a_{\eta_0}\rangle & \subset & \langle a_{\eta_0}, a_{\eta_1}\rangle & \subset & \langle a_{\eta_0}, a_{\eta_1}, a_{\eta_2}\rangle & \subset & \dots \end{array}$$

of finitely generated ideals, which by (II) is really a strictly ascending chain of principal ideals

$$\langle 0\rangle \subset \langle b_1\rangle \subset \langle b_2\rangle \subset \langle b_3\rangle \subset \dots$$

which must stabilize at b_n for some $n \in \omega$ by lemma(ii.). Since we constructed this sequence of ideals to be strictly increasing, our subsequence $\{a_{\eta_\iota}\}_{\iota\in\beta}$ must then end at a_{η_n}, *i.e.* $\beta = n+1$. Hence

$$\langle b_n\rangle = \left\langle a_{\eta_\gamma}\right\rangle_{\gamma\in(n+1)} = \langle a_\eta\rangle_{\eta\in\alpha} = I$$

is finitely generated (moreover principal).

3. We prove $\mathbb{Z}[i]$ is a Euclidean domain, hence also a PID and a UFD. Its norm is given by the restriction of abs on $\mathbb{C}$ to $\mathbb{Z}[i]$, *i.e.*

$$|x+yi| = x^2+y^2$$

Clearly this norm maps $Z[i]\setminus\{0\}$ to positive integers. We also know that $|\cdot|$ is multiplicative. We can prove that $|\cdot|$ satisfies the conditions to make $\mathbb{Z}[i]$ into a Euclidean domain by the example in Dummit and Foote 3rd edition page 272. I will write out the core high level procedure of this proof to show I understand it, but I will skip the computational details since I will just be mostly transcribing from Dummit and Foote if I do that.

Given $\alpha,\beta \in \mathbb{Z}[i]$, we can choose the best quotient candidate to be the $\sigma \in \mathbb{Z}[i]$ that is closest in absolute value to the actual quotient $\frac{\alpha}{\beta}$ in the field of fraction $\mathbb{Q}[i]$. Then the remainder γ, where $\alpha = \beta\sigma + \gamma$, is given by the identity

$$\gamma = \left(\frac{\alpha}{\beta} - \sigma\right)\beta$$

Then by our choice of choosing the nearest lattice point for σ, we have that $\left(\frac{\alpha}{\beta} - \sigma\right)$ must have norm not exceeding $\frac{1}{2}$, so by multiplicativity of the complex norm we know that the norm of γ is less than the norm of β.

For an element $a + bi \in \mathbb{Z}[i]$ to be a unit, it has to have an inverse w. Then by multiplicativity of the norm we have the equation

$$(a^2 + b^2)|w| = |(a + bi)w| = |1| = 1$$

and since $|w| \in \mathbb{Z}$ this implies $a^2 + b^2 = 1$. Then because a^2 and b^2 can both only be natural numbers, we have the four cases for what $a + bi$ can equal: 1, -1, i, $-i$.

4. Running the Euclidean algorithm on 85 and $1 + 13i$, we get

$$85 = (-6i)(1 + 13i) + (7 + 6i) \tag{1}$$
$$1 + 13i = (1 + i)(7 + 6i) \tag{2}$$

By theorem 4 in §8.1 of Dummit and Foote we know that the last nonzero remainder is a gcd, so a gcd of 85 and $1 + 13i$ is $7 + 6i$. The linear combination is

$$7 + 6i = 1(85) + 6i(1 + 13i)$$

5. Define the norm N on $\mathbb{Z}[\sqrt{10}]$ by

$$N(a + b\sqrt{10}) \coloneqq |a^2 - 10b^2|$$

This norm always takes integer values. Notice

$$\begin{aligned}
&N((a + b\sqrt{10})(c + d\sqrt{10})) \\
&= N((ac + 10bd) + (ad + bc)\sqrt{10}) \\
&= |a^2c^2 + 2(10)abcd + 10^2b^2d^2 - 10a^2d^2 - (10)2abcd - 10b^2c^2| \\
&= |a^2c^2 - 10a^2d^2 - 10b^2c^2 + 10^2b^2d^2| \\
&= |a^2 - 10b^2|\,|c^2 - 10d^2| \\
&= N(a + b\sqrt{10})N(c + d\sqrt{10})
\end{aligned}$$

Hence this norm is also multiplicative. Now consider that we can write 10 as two different products

$$\sqrt{10} \cdot \sqrt{10} = 10 = 2 \cdot 5$$

$\sqrt{10}$ has norm 10, 2 has norm 4, 5 has norm 25. Now, nothing in $\mathbb{Z}[\sqrt{10}]$ can have norm 2 because $|a^2 - 10b^2| = 2$ requires either $a^2 - 10b^2 = 2 \implies a^2 \equiv 2 \mod 10$ or $-a^2 + 10b^2 = 2 \implies a^2 \equiv 8 \mod 10$, both of which are impossible just by casework. Therefore none of these factors can have a smaller factor with norm 2, so for $\sqrt{10}$ and 2 this means that they can have no smaller irreducible factors. But then these two factorizations of 10 into irreducibles (whether or not 5 is irreducible is irrelevent, as the other factors already mismatch) are different, showing $\mathbb{Z}[\sqrt{10}]$ is not a UFD.

6. Denote the ideal we take quotient using by I and denote the quotient ring itself as R. I will use the same constants and ring operations from the parent space $\mathbb{Q}[x, y]$ to represent their images in the quotient by default, and the symbols will only refer to the original entities of the parent space if I specify so explicitly.

The quotient relation gives us $x^2 + y^2 = 1$, from which we deduce

$$x^2 = (1 - y)(1 + y)$$

First, I claim that x is irreducible. Suppose $pq = x$. Then in the parent space $pq = x + r(x^2 + y^2 - 1)$ for some polynomial r. Yeah OK. And then I also claim $x \nmid (1 - y)$ and $x \nmid (1 + y)$, showing x is not prime and so R is not a UFD. But I don't actually know how to prove that x is irreducible, so I give up.