Math 100B: Homework 5

Merrick Qiu

Problem 1

Let $f, g \in R$ and we want to show $f = gq + r$ with $q, r \in R$ and $N(r) < N(g)$. Since $R \subset \mathbb{C}$, we can write $\frac{f}{g} = q + \frac{r}{g}$ in $\mathbb{C}$. If $N(\frac{r}{g}) < 1$, then $N(r) < N(g)$ due to the multiplicativity of the norm.

The elements of R form a rectangular grid of side length 1 and $\sqrt{2}$ inside of $\mathbb{C}$. Therefore for any $\frac{f}{g} \in \mathbb{C}$, we can find a $q \in R$ that is at most $\frac{\sqrt{3}}{2} < 1$ away from $\frac{f}{g}$. Therefore $N(\frac{f}{g} - q) = N(\frac{r}{g}) < 1$ in the equation $\frac{f}{g} = q + \frac{r}{g}$. Multiplying by g on both sides, we get $f = gq + r$ with $N(r) < N(g)$.

Since R is a Euclidean domain, it is also a PID and a UFD.

Problem 2

(a) If $2 = xy$ then $N(2) = N(x)N(y)$. $N(2) = 4$ so $N(x) = N(y) = 2$ if 2 was reducible. However there does not exist any $x = a + b\sqrt{2}$ such that $a^2 - db^2 = 2$ when $d \leq 3$ so 2 is irreducible.

(b) If $d = 2n$ is even then $2n = d = \sqrt{d}\sqrt{d}$ but 2 does not divide $\sqrt{d}$ so 2 is not prime. If $d = 2n + 1$ is odd then $-2n = 1 - d = (1 + \sqrt{d})(1 - \sqrt{d})$ but 2 does not divide $1 + \sqrt{d}$ or $1 - \sqrt{d}$ so 2 is not prime. Therefore R is not a UFD.

Problem 3

(a) If $p = a^2 + 2b^2$, then it can be written as the product $p = (a + b\sqrt{-2})(a - b\sqrt{2})$. Since $N(a + b\sqrt{-2}) = N(a - b\sqrt{-2}) = p$, both these elements are irreducible.

If p cannot be written as $p = a^2 + 2b^2$ then p is irreducible in R. If it was reducible, then $p = xy$ and $N(x) = N(y) = p$. However if $x = a + b\sqrt{-2}$ then $N(x) = a^2 + 2b^2$ which is a contradiction.

(b) We can write $2 = 0^2 + 2(1)^2$ so 2 falls into case (ii). For the case when $p \equiv 5 \mod 8$ or $p \equiv 7 \mod 8$, notice that $a^2 = 0, 1, 4 \mod 8$ and $2b^2 = 0, 2 \mod 8$ so $a^2 + 2b^2 = 0, 1, 3, 4, 6 \mod 8$. so it is not possible to write $p = a^2 + 2b^2$.

Problem 4

We can write

$$\begin{aligned}
1122 &= (2)(3)(11)(17) \\
&= \left[(0+\sqrt{-2})(0-\sqrt{-2})\right]\left[(1+\sqrt{-2})(1-\sqrt{-2})\right]\left[(3+\sqrt{-2})(3-\sqrt{-2})\right]\left[(3+2\sqrt{-2})(3-2\sqrt{-2})\right]
\end{aligned}$$

Therefore we can write $1122 = \gamma\overline{\gamma}$ where gamma is the product with four of the factors selected above in the following ways. Due to symmetry we can choose $(0+\sqrt{-2})$ as our first factor.

$$\begin{aligned}
\gamma &= (0+\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})(3+2\sqrt{-2}) = -28-13\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})(3-2\sqrt{-2}) = -20+19\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1+\sqrt{-2})(3-\sqrt{-2})(3+2\sqrt{-2}) = -32+7\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1+\sqrt{-2})(3-\sqrt{-2})(3-2\sqrt{-2}) = 8+23\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1-\sqrt{-2})(3+\sqrt{-2})(3+2\sqrt{-2}) = -8+23\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1-\sqrt{-2})(3+\sqrt{-2})(3-2\sqrt{-2}) = 32+7\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1-\sqrt{-2})(3-\sqrt{-2})(3+2\sqrt{-2}) = 20+19\sqrt{-2} \\
\gamma &= (0+\sqrt{-2})(1-\sqrt{-2})(3-\sqrt{-2})(3-2\sqrt{-2}) = 28-13\sqrt{-2}
\end{aligned}$$

$$\begin{aligned}
1122 &= (-28-13\sqrt{-2})(-28+13\sqrt{-2}) = 28^2+2\cdot 13^2 \\
1122 &= (-20+19\sqrt{-2})(-20-19\sqrt{-2}) = 20^2+2\cdot 19^2 \\
1122 &= (-32+7\sqrt{-2})(-32-7\sqrt{-2}) = 32^2+2\cdot 7^2 \\
1122 &= (8+23\sqrt{-2})(8-23\sqrt{-2}) = 8^2+2\cdot 23^2
\end{aligned}$$

These are the only ways to write 1122 as a^2+2b^2 since R is a UFD and the existence of a another way would imply a different factorization of 1122.

Problem 5

(a) First we show that $\mathbb{Z}[\sqrt{-2}]/(p)$ is a field. The evaluation homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-2}]$ that sends $x \to \sqrt{-2}$ has $(x^2+2) \subseteq \ker\phi$. To show the converse containment, notice that when $f \in \ker\phi$, $f = (x^2+2)q + r$ with $\deg r < x^2+2$. But there exists no $r \in \ker\phi$ with $\deg r < x^2+2$ so $r = 0$ and $(x^2+2) = \ker\phi$. By the first isomorphism theorem, $\mathbb{Z}[\sqrt{-2}] \cong \mathbb{Z}[x]/(x^2+2)$. Since (p) is irreducible in the Euclidean domain $\mathbb{Z}[\sqrt{-2}]/(p)$, it is maximal. By the correspondence theorem, $\mathbb{Z}[\sqrt{-2}]/(p)$ can only have two ideals so it is a field.

We can write

$$\begin{aligned}
\mathbb{Z}[\sqrt{-2}]/(p) &\cong \frac{\mathbb{Z}[x]/(x^2+2)}{(p, x^2+2)/(x^2+2)} \\
&\cong \mathbb{Z}[x]/(p, x^2+2) \\
&\cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^2+2)}
\end{aligned}$$

Elements in $\frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^2+2)}$ are degree 1 polynomials in $\mathbb{Z}/p\mathbb{Z}$, so there are p^2 elements in the field.

(b) Since $p = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$, b is invertible modulo p since b is nonzero(if b is zero, then $p = a^2$ which is a contradiction since p is prime). Solving for -2 in the equation $a^2 \equiv -2b^2 \mod p$ gives us that that $\left(\frac{a}{b}\right)^2 = -2$. Therefore $x^2 + 2 = (x - \frac{a}{b})(x + \frac{a}{b})$ and so by the chinese remainder theorem and then evaluating at $x = \pm\frac{a}{b}$, we get

$$\begin{aligned}
\mathbb{Z}[\sqrt{-2}]/(p) &\cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^2+2)} \\
&\cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x - \frac{a}{b})} \times \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x + \frac{a}{b})} \\
&\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}
\end{aligned}$$

At the same time,

$$\mathbb{Z}[\sqrt{-2}]/(p) \cong \mathbb{Z}[\sqrt{-2}]/(a - b\sqrt{-2}) \times \mathbb{Z}[\sqrt{-2}]/(a + b\sqrt{-2})$$

Therefore by matching the rings in the ring product we get that

$$\mathbb{Z}[\sqrt{-2}]/(a + b\sqrt{-2}) \cong \mathbb{Z}/p\mathbb{Z}.$$