David Beydler
MATH 540B
Due: 1/16/08

HW #1

$\boxed{8.1}$ 3) [Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.]

(In retrospect, I suppose we didn't have to divide by an arbitrary number, just by 1.)

Pf: Let $x \in R$ be nonzero such that $N(x) = m$.
Let $y \in R$ be arbitrary. $\longrightarrow$ Let's divide y by x.
Since R is a Euclidean Domain, we can do this to get:
$y = qx + r$, where $q, r \in R$ and $N(r) < N(x) = m$.
Now suppose r is nonzero. Then we get a contradiction right away, since $N(r) < m$, and m is supposed to be the minimum norm of nonzero elements of R. So, we must have that $r = 0$, so $y = qx$. This works for all nonzero y, including $y = 1$. So, $\exists q_1 \in R$ such that $1 = q_1 x$. Thus, x is a unit.

(Thanks to Ben for help on this part)

Suppose we have a nonzero element, $z \in R$, such that $N(z) = 0$. Then the minimum norm of nonzero elements of R is 0 (i.e. $m = 0$). Thus, by above work, z is a unit. ☒

(from sheet)

1) [Consider the integral domain $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ where d is a nonzero, square-free integer. Let $N(a+b\sqrt{d}) = a^2 - db^2$.]

a) [Prove that $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\sqrt{d}]$.]

Pf: Let $x = a_1 + b_1\sqrt{d}$ and $y = a_2 + b_2\sqrt{d}$. Then,

$$\begin{aligned}
N(xy) &= N\big((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})\big) \\
&= N\big(a_1a_2 + a_1b_2\sqrt{d} + b_1a_2\sqrt{d} + b_1b_2d\big) \\
&= (a_1a_2 + b_1b_2d)^2 - d(a_1b_2 + b_1a_2)^2 \\
&= a_1^2a_2^2 + \cancel{2a_1a_2b_1b_2d} + b_1^2b_2^2d^2 - (a_1^2b_2^2d + \cancel{2a_1a_2b_1b_2d} + a_2^2b_1^2d) \\
&= a_1^2a_2^2 - (a_1^2b_2^2 + a_2^2b_1^2)d + b_1^2b_2^2d^2 \\
&= (a_1^2 - b_1^2d)(a_2^2 - b_1^2d) \\
&= N(a_1 + b_1\sqrt{d})\,N(a_2 + b_2\sqrt{d}) \\
&= N(x)N(y). \quad \blacksquare
\end{aligned}$$

(Thanks to Ben and Sergio for help on $(\Leftarrow)$)

b) [Show that $x \in \mathbb{Z}[\sqrt{d}]$ is a unit iff $N(x) = \pm 1$.]

Pf: $(\Rightarrow)$ Suppose $x \in \mathbb{Z}[\sqrt{d}]$ is a unit. Then $\exists y \in \mathbb{Z}[\sqrt{d}]$ with $xy = 1$. So, $N(xy) \underset{\text{by (a)}}{=} N(x)N(y) = N(1) = 1$.

Thus $N(x) = \pm 1$.

$(\Leftarrow)$ Suppose $N(x) = \pm 1$, where $x = a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$. Then $a^2 - db^2 = \pm 1$. If $N(x) = 1$, then consider $y = a - b\sqrt{d}$. Here, $xy = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d = 1$, so x is a unit. If $N(x) = -1$, then consider $y = -a + b\sqrt{d}$. Here, $xy = (a + b\sqrt{d})(-a + b\sqrt{d}) = -a^2 + b^2d = -(a^2 - b^2d) = -(-1) = 1$, so again x is a unit.

$\blacksquare$

DB3

(1 cont)

c) [Show that if $N(x) = \pm p$ where p is a prime, then x is irreducible in $\mathbb{Z}[\sqrt{d}]$.]

Pf: (by contradiction) Suppose that $N(x) = \pm p$, where p is a prime, and that x is reducible in $\mathbb{Z}[\sqrt{d}]$. Then $\exists u, v \in R$ s.t. u and v are not units and $x = uv$. But, $\pm p = N(x) = N(uv) = N(u)N(v)$, so $N(u) | p$ or $N(v) | p$. WLOG, suppose that $N(u) | p$. Then $N(u) = \pm p$ or $N(u) = \pm 1$. If $N(u) = \pm 1$, then u is a unit (by part (b)), a contradiction. If $N(u) = \pm p$, then $N(v) = \pm 1$, so v is a unit, again a contradiction. So, x is irreducible in $\mathbb{Z}[\sqrt{d}]$. ∎

d) [Find all the units in $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$.]

Let $x = a + bi \in R$ be a unit. Then,

$$N(x) = N(a+bi) = a^2 + b^2 \underset{\text{by (b)}}{=} \pm 1$$

So, $a = \pm 1$ or $b = \pm 1$. Thus, $\boxed{x = \pm 1 \text{ or } x = \pm i}$.

e) [One can show that $\mathbb{Z}[i]$ is a UFD. Why doesn't the following contradict this fact?

$$10 = (1+i)(1-i)(2-i)(2+i) = (-1-i)(-1-i)(1+2i)(-2-i)$$

Hint: Think about units.]

Each factor can be paired with an associate as follows:

$(1+i) = (-i)(-1-i)$

$(1-i) = (-i)(-1-i)$

$(2-i) = (i)(1+2i)$

$(2+i) = (-1)(-2-i)$

Thus the factorizations are not unique.