Unusual Integral Domains
by William Gasarch

1 Basic Definitions

Def 1.1 Let D be an integral domain and U be its units.

1. $x \in \mathsf{D} - \mathsf{U}$ is *irreducible* if
$$x = ab \Rightarrow a \in U orb \in U.$$
2. $x \in \mathsf{D} - \mathsf{U}$ is *prime* if
$$x|ab \Rightarrow x|a \vee x|b.$$
3. x is *composite* if $x \notin \mathsf{U} \cup \{0\}$ and x is not prime.
4. *Note:* D is the disjoint union of Zero, Units, Primes, and Composites.

2 The Domain $\mathsf{Z}[\sqrt{-d}]$ and Norms

Def 2.1 Let $d \in \mathsf{N}$ be square free. Let $\mathsf{D} = \mathsf{Z}[\sqrt{-d}]$. Then we define the *norm on* D to be the function $f : \mathsf{D} \rightarrow \mathsf{N}$
$$f(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2 d.$$

Theorem 2.2 *Let $d \in \mathsf{N}$ be square free. Let $\mathsf{D} = \mathsf{Z}[\sqrt{-d}]$. Let $x, y \in \mathsf{D}$.*

1. *$f(xy) = f(x)f(y)$.*
2. *x is a unit iff $f(x) = 1$.*
3. *If $f(x)$ is a prime then x is irreducible.*
4. *If $x \in \mathsf{D} - \mathsf{U}$ is composite and $N(x) = pq$ where p, q are primes, then p and q are squares mod d.*

5. *If $N(x) = pq$ where p, q are primes, and at least one of p, q is not a squares mod d, then x is irreducible. (This is just the contrapositive of the last item.)*

6. *If y divides x then $N(y)$ divides $N(x)$.*

Proof:
1) Let $x = a_1 + b_1\sqrt{-d}$ and $y = a_2 + b_2\sqrt{-d}$.

$$f(x) = a_1^2 + b_1^2 d$$

$$f(y) = a_2^2 + b_2^2 d$$

$$f(x)f(y) = (a_1a_2)^2 + ((a_1b_2)^2 + (a_2b_1)^2))d + (b_1b_2d)^2$$

$$xy = a_1a_2 - b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{-d}$$

$$f(xy) = (a_1a_2 - b_1b_2d)^2 + (a_1b_2 + a_2b_1)^2 d$$

$$= (a_1a_2)^2 - 2a_1a_2b_1b_2d + (b_1b_2d)^2 + (a_1b_2)^2 d + 2a_1a_2b_1b_2d + (a_2b_1)^2 d$$

$$= (a_1a_2)^2 + (b_1b_2d)^2 + (a_1b_2)^2 d + (a_2b_1)^2 d$$

$$= (a_1a_2)^2 + ((a_1b_2)^2 + (a_2b_1)^2)d + (b_1b_2d)^2 = f(x)f(y).$$

2) If $x \in \mathsf{U}$ then there exists $y \in \mathsf{U}$ such that $xy = 1$
$xy = 1$
$f(xy) = f(1) = 1$
$f(x)f(y) = 1.$
Hence $f(x) = f(y) = 1.$

3) Assume $x = yz$. Then
$f(x) = f(yz) = f(y)f(z)$

Since $f(x)$ is prime either $f(y) = 1$ or $f(z) = 1$. Hence one of y, z is a unit.

4) Let $x = yz$ where $y, z \in \mathsf{D} - \mathsf{U}$.

$f(x) = f(yz) = f(y)f(z)$. But note that $f(x) = pq$ where p, q are primes. Hence $f(y)f(z) = pq$. Since $y, z \notin \mathsf{U}$ we must have $f(y) = p$ and $f(z) = q$.

Let $y = a_1 + b_1\sqrt{-d}$ and $z = a_2 + b_2\sqrt{-d}$. Hence

$f(y) = a_1^2 + db_1^2$ and $f(z) = a_2^2 + db_2 62$ hence

$p = a_1^2 + db_1^2$ and $q = a_2^2 + db_2 62$. Take these mod d to get

$p \equiv a_1^2 \pmod{d}$, $q \equiv a_2^2 \pmod{d}$.

6) Let $x = yz$. Then $N(x) = N(y)N(z)$. Hence $N(y)$ divides $N(x)$.

∎

3 Irreducibles and Primes

Theorem 3.1

1. *Let* D *be any integral domain. If* x *is prime in* D *then* x *is irreducible in* D.

2. *There exists integral domains where there are irreducibles that are not prime.*

Proof:

1) Let $x = yz$. Then x divides yz. Since x is prime either x divides y or x divides z. We assume x divides y (the other case is similar). Hence $y = xw$. Hence

$x = yz = xwz$, so $xwz - x = x(wz - 1) = 0$. Since D is an integral domain either $x = 0$ (which is it not) or $wz - 1 = 0$, so $wz = 1$. Hence z is a unit.

2) Let $\mathsf{D} = \mathsf{Z}[\sqrt{-5}]$. Note that the squares mod 5 are $\mathrm{SQ}_5 = \{1, 4\}$.

We use Theorem 2.2.5 and 2.2.7 to show several elements of $\mathsf{D} - \mathsf{U}$ are irreducible, and that they do not divide each other.

- 2 is irredubicle: $f(2) = 4 = 2 \times 2$ and $2 \notin \mathrm{SQ}_5$.
- 3 is irredubicle: $f(3) = 9 = 3 \times 3$ and $3 \notin \mathrm{SQ}_5$.

- $1+\sqrt{-5}$ is irreducible: $f(1+\sqrt{-5}) = 6 = 2 \times 3$, but $2, 3 \notin \mathrm{SQ}_5$.
- $1-\sqrt{-5}$ is irreducible: $f(1+\sqrt{-5}) = 6$, but $2, 3 \notin \mathrm{SQ}_5$.
- $2 \not| 1+\sqrt{-5}$: $N(2) = 4$, $N(1+\sqrt{-5}) = 6$, but $4 \not| 6$.
- $1+\sqrt{-5} \not| 2$: $N(1+\sqrt{-5}) = 6$, $N(2) = 4$, but $6 \not| 4$.
- $2 \not| 1-\sqrt{-5}$: $N(2) = 4$, $N(1-\sqrt{-5}) = 6$, but $4 \not| 6$.
- $1-\sqrt{-5} \not| 2$: $N(1+\sqrt{-5}) = 6$, $N(2) = 4$, but $6 \not| 4$.
- $3 \not| 1+\sqrt{-5}$: $N(3) = 9$, $N(1+\sqrt{-5}) = 6$, but $9 \not| 6$.
- $1+\sqrt{-5} \not| 3$: $N(1+\sqrt{-5}) = 6$, $N(3) = 9$, but $6 \not| 9$.
- $3 \not| 1+\sqrt{-5}$: $N(3) = 9$, $N(1+\sqrt{-5}) = 6$, but $9 \not| 6$.
- $1+\sqrt{-5} \not| 3$: $N(1-\sqrt{-5}) = 6$, $N(3) = 9$, but $6 \not| 9$.
- $3 \not| 1+\sqrt{-5}$: $N(3) = 9$, $N(1+\sqrt{-5}) = 6$, but $9 \not| 6$.
- $3 \not| 1+\sqrt{-5}$: $N(3) = 9$, $N(1-\sqrt{-5}) = 6$, but $9 \not| 6$.

This is far more than we need. However, we now have the following:

- 2 divides $6 = (1+\sqrt{-5})(1-\sqrt{5})$.
- But 2 does not divide $1+\sqrt{-5}$ or $1-\sqrt{5})$.
- Hence 2 is not prime.

So 2 is irreducible but not prime. Same for $3, 1+\sqrt{5}$, $1-\sqrt{5}$. ▮

4 What Do We Mean By *An Infinite Number of Irreducibes*

If we are looking at primes in Z do we count 7 and -7 as two primes or one? We count them as one prime. The key is that their ratio is a unit.

Convention 4.1 Let E be the following equivalence on irreducibles: $E(x, y)$ iff $x/y \in \mathsf{U}$.