**Math 403 Chapter 18: Irreducibles, Associates, Primes, UFDs**

1. **Introduction:** In terms of structures we've basically gone from rings in general to integral domains to fields. However within integral domains there is a lot of interesting variation.

2. **Associates, Irreducibles, and Primes**

   (a) **Definition:** Suppose $D$ is an integral domain and $a, b \in D$. Then $a$ and $b$ are *associates* if $a = ub$ for some unit $u$.

   **Example:** In $\mathbb{Z}$, $a = 5$ and $b = -5$ are associates because $5 = (-1)(-5)$ and $-1$ is a unit.

   **Example:** In $\mathbb{Q}$ every pair of nonzero rationals are associates.

   **Example:** In $\mathbb{Z}[i]$, $a = -1 + i$ and $b = 1 + i$ are associates because $-1 + i = (i)(1 + i)$ and $i$ is a unit.

   (b) **Definition:** Suppose $D$ is an integral domain and $a \in D$ is a nonzero non-unit. Then $a$ is a *reducible* if we may write $a = bc$ for $b, c \in D$ and neither $b$ nor $c$ a unit. Conversely $a$ is an *irreducible* if whenever we write $a = bc$ with $bc \in D$ then one of $b$ or $c$ must be a unit.

   **Note:** The term *reducible* is not used in the book but I like it, so I'm using it.

   **Example:** In $\mathbb{Z}$, $a = -6$ is reducible because $-6 = (2)(-3)$ and neither 2 nor $-3$ is a unit.

   **Example:** In $\mathbb{Z}$, $a = -7$ is irreducible because we can only write $-7 = (-1)(7)$ or $-7 = (1)(-7)$ and in both cases one is a unit.

   (c) **Definition:** Suppose $D$ is an integral domain and $a \in D$ is a nonzero non-unit. Then $a$ is *prime* if whenever $a \mid bc$ for $b, c \in D$ we must have $a \mid b$ or $a \mid c$.

   **Example:** In $\mathbb{Z}$, $a = 6$ is not prime because $6 \mid (3)(4)$ but $6 \nmid 3$ and $6 \nmid 4$.

   **Example:** In $\mathbb{Z}[\sqrt{-3}]$ the element $1 + \sqrt{-3}$ is not prime. To see this, observe that $1 + \sqrt{-3} \mid (2)(2)$ because $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4$ However $1 + \sqrt{-3} \nmid 2$ because if it did we would have some $a + b\sqrt{-3}$ with $(1 + \sqrt{-3})(a + b\sqrt{-3}) = 2$. FOILing the left and solving for $a, b$ shows that no such $a, b \in \mathbb{Z}$ exist.

**Note:** Be careful. In $\mathbb{Z}^+$ the term *prime* is used instead of *irreducible* and the term *irreducible* is not used. This is because the two mean the same thing in $\mathbb{Z}^+$. However in general they don't. Specifically the following two theorems clarify:

   (d) **Theorem:** In an integral domain every prime is irreducible.

   **Proof:** Suppose $a \in D$ is prime and $a = bc$. We claim that one of $b, c$ is a unit. Since $a = bc$ we know $a \mid bc$ and since $a$ is prime without loss of generality let's say $a \mid b$. Then $b = a\alpha$ for some $\alpha \in D$, so then $b = a\alpha = bc\alpha$ and then we cancel the $b$ (which we may do in an integral domain) to get $1 = c\alpha$ so that $c$ is a unit. $\mathcal{QED}$

   (e) **Theorem:** In a principal ideal domain every irreducible is prime.

   **Proof:** Suppose $a \in D$ is irreducible and $a \mid bc$. We claim $a \mid b$ or $a \mid c$. Consider the ideal $\langle a, b \rangle$. Since $D$ is a PID we then have $\langle a, b \rangle = \langle d \rangle$ for some $d \in D$. Since $a \in \langle a, b \rangle = \langle d \rangle$ we have $a = d\alpha$ for some $\alpha \in D$ and since $a$ is irreducible either $d$ or $\alpha$ is a unit.

   If $d$ is a unit then $\langle a, b \rangle = \langle d \rangle = D$ and so $1 = ax + by$ for some $x, y \in D$ so then $c = acx + bcy$. Then since $a \mid acx$ and $a \mid bcy$ we have $a \mid c$.

   If $\alpha$ is a unit then $\langle a \rangle = \langle d \rangle = \langle a, b \rangle$ and so we have $b = a\beta$ for some $\beta \in D$ so then $a \mid b$ $\mathcal{QED}$

   **Note:** The ring $\mathbb{Z}$ is a PID (can you prove this?) which is why the terms *irreducible* and *prime* can be used interchangeably.

To help look at some more interesting integral domains it can be helpful to define the norm:

(f) **Definition:** Let $d \in \mathbb{Z}$ with $d \neq 1$ and $d$ is square-free (not divisible by any square). In the integral domain $\mathbb{Z}[\sqrt{d}]$ we define the *norm* by $N(a + b\sqrt{d}) = |a^2 - db^2|$. It is fairly straightfoward to show that:

- $N(x) = 0$ iff $x = 0$.
- $N(xy) = N(x)N(y)$.
- $N(x) = 1$ iff $x$ is a unit.

Note that $N$ maps to $\mathbb{Z}^+$ and so the behavior is predictable in the range as we see in this next example.

**Example:** In $\mathbb{Z}[\sqrt{-3}]$ the element $1 + \sqrt{-3}$ is irreducible. To see this suppose that $1 + \sqrt{-3} = xy$ with neither $x$ nor $y$ a unit. Then $N(x)N(y) = N(xy) = N(1 + \sqrt{-3}) = 4$ and since both $N(x), N(y) \in \mathbb{Z}^+$ we must have $N(x) = N(y) = 2$ (since $x$ and $y$ are not units). If $x = a + b\sqrt{-3}$ then $N(a + b\sqrt{-3}) = a^2 + 3b^2 = 2$ which is impossible for $a, b \in \mathbb{Z}$.

3. **Unique Factorization Domains**

(a) **Definition:** An integral domain $D$ is a *unique factorization domain* (UFD) if every nonzero non-unit in $D$ can be written as a product of irreducibles in $D$ and the factorization is unique up to order and associates.

**Note:** The prototypical example is $\mathbb{Z}$. In $\mathbb{Z}^+$ we are well-aware that we can uniquely factor up to order, for example $315 = (3)(3)(5)(7)$ and all of $3, 5, 7$ are irreducible (same as prime in $\mathbb{Z}$). Extending to $\mathbb{Z}$ just means we can swap out irreducibles with associates, for example $315 = (-3)(3)(-5)(7)$, and we wouldn't consider it different. Also we wouldn't consider $315 = (3)(3)(5)(7)(1)(-1)(-1)$ different, either.

**Example:** $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Observe that $6 = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. This is not crazy obvious, we need to show that both factorizations are into irreducibles and that the two factorizations are not up to associates.

(b) **Theorem:** Every PID is a UFD.
**Proof:** Omit, lengthy. $\mathcal{QED}$

(c) **Corollary:** If $F$ is a field then $F[x]$ is a UFD.
**Proof:** We proved that $F[x]$ is a PID and then the result follows. $\mathcal{QED}$