Primes in Computable UFDs

Joe Mileti
Grinnell College

April 10, 2013

Units and Associates

Definition

An integral domain is a commutative ring with identity such that whenever $ab = 0$, either $a = 0$ or $b = 0$.

Definition

Let A be an integral domain. An element $u \in A$ is called a unit if there exists $w \in A$ with $uw = 1$. We let $U(A)$ be the set of units of A.

Definition

Let A be an integral domain and let $a, b \in A$. We say that a and b are associates if there exists $u \in U(A)$ with $au = b$. Equivalently, both $a \mid b$ and $b \mid a$.

Units

Proposition

Let A be an integral domain.

- *$U(A)$ is a multiplicative group.*
- *If $a \in U(A)$ and $b \mid a$, then $b \in U(A)$.*

For example, consider the integral domain $\mathbb{Z}[\sqrt{2}]$. Notice that $1 + \sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$ because $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$. Taking powers of $1 + \sqrt{2}$, the following are units:

- $3 + 2\sqrt{2}$
- $7 + 5\sqrt{2}$
- $17 + 12\sqrt{2}$

In fact, $U(\mathbb{Z}[\sqrt{2}]) = \{\pm(1 + \sqrt{2})^n : n \in \mathbb{Z}\}$.

Primes and Irreducibles

Definition

Let A be an integral domain. Let $p \in A \backslash U(A)$ be nonzero.

- p is irreducible if whenever $p = ab$, either a is a unit or b is a unit.
- p is prime if whenever $p \mid ab$, either $p \mid a$ or $p \mid b$.

In an integral domain, primes are always irreducible but the converse need not hold. In $\mathbb{Z}[\sqrt{-5}]$ we have

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

All factors are irreducible but none are prime.

UFDs

Definition

A unique factorization domain or UFD is an integral domain A such that:

- Every (nonzero nonunit) element of A can be written as a product of irreducibles.
- Any representation of an element as a product of irreducibles is unique up to order and associates.

In $\mathbb{Z}[i]$, we have

$$(2+i)(2-i) = 5 = (1+2i)(1-2i)$$

but $2+i = i \cdot (1-2i)$ and $2-i = (-i) \cdot (1+2i)$.

UFDs

Proposition

In a UFD, every irreducible is prime.

Proposition

Let A be an integral domain. The following are equivalent.

- *A is a UFD.*
- *Every element is a product of irreducibles, and every irreducible is prime.*
- *The strict divisibility relation is well-founded, and every irreducible is prime.*

Examples of UFDs

Theorem
$\mathbb{Z}$ is a UFD.

To prove this, one shows that every element is a product of irreducibles by induction. One then develops enough properties of GCD's (i.e. that they exist and can be written as a linear combination of the elements) to prove that irreducibles are prime. These arguments carry over to the following.

Theorem

- *In a Euclidean domain, all irreducible elements are prime.*
- *In a PID, all irreducible elements are prime.*

Noetherian Rings

Definition

A ring is Noetherian if it has no strictly ascending sequence of ideals. This is equivalent to the statement that every ideal is finitely generated.

Since $a \mid b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$, the strict divisibility relation is well-founded in any Noetherian integral domain.

Corollary

Let A be a Noetherian integral domain. If every irreducible element is prime, then A is a UFD.

Corollary

Euclidean domains and PIDs are UFDs.

Structure of $\mathbb{Z}[\sqrt{q}]$

Theorem
$\mathbb{Z}[i]$ is a UFD and $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Theorem
Let $q \in \mathbb{Z}$ be prime.

- *If $q < 0$, then $U(\mathbb{Z}[\sqrt{q}]) = \{1, -1\}$.*
- *If $q > 0$, then $U(\mathbb{Z}[\sqrt{q}])$ is infinite.*

Theorem
$\mathbb{Z}[\sqrt{-2}]$ is a UFD, but $\mathbb{Z}[\sqrt{q}]$ is not a UFD whenever $q < -2$ is prime.

The situation for $q > 0$ is much more complicated.

Primes in $\mathbb{Z}[i]$

Theorem

Let $p \in \mathbb{Z}$ be an odd prime. The following are equivalent:

- *p is not prime in $\mathbb{Z}[i]$.*
- *-1 is a square modulo p.*
- *$p \equiv 1 \pmod 4$.*

Furthermore, these are all equivalent to p being a sum of two squares in $\mathbb{Z}$.

For example,

- $13 \mid (5+i)(5-i)$ or $13 = (3+2i)(3-2i)$.
- $5^2 \equiv -1 \pmod{13}$.
- $13 \equiv 1 \pmod 4$.

and $13 = 3^2 + 2^2$.

Primes in $\mathbb{Z}[\sqrt{q}]$

Theorem

Let $q \in \mathbb{Z}$ be prime. Let $p \in \mathbb{Z}$ be an odd prime with $p \neq q$. The following are equivalent:

- *p is not prime in $\mathbb{Z}[\sqrt{q}]$.*
- *q is a square modulo p.*

In particular, by introducing a simple factorization for q, we may do the following:

- Lose the property of being a UFD.
- Destroy other primes.
- Introduce new units.

Primes in Computable UFDs

Let p_i be the i^{th} prime in $\mathbb{N}$.

Theorem (Dzhafarov, Mileti)

Let Q be a Π^0_2 set. There exists a computable UFD A such that:

- *$\mathbb{Z}$ is a subring of A.*
- *p_i is prime in A if and only if $i \in Q$.*

Corollary

There exists a computable UFD A such that the set of primes is Π^0_2-complete in every computable presentation of A (even uniformly in an index for the presentation).

Bad Presentations

Many constructions in computable algebra build a "bad" computable copy of a "nice" ring where the objects one is considering are complicated.

Theorem (Friedman, Simpson, Smith)

- *There is a computable local ring such that the unique maximal ideal M satisfies $M \geq_T 0'$.*
- *There is a computable ring such that P has PA-degree for every prime ideal P.*

These constructions start in $\mathbb{Q}[x_1, x_2, x_3, \ldots]$ and use the algebraically independent elements to do the coding. Infinitely many x_i do some coding, and infinitely many do not.

Idea

We want to turn primes on and off based on a Π^0_2 occurrence. So if i acts infinitely often, we want p_i to be prime in the end. If i acts finitely often, we want it not to be prime.

To work for i, we assume finite action, and introduce a factorization $p_i = xy$ for new elements x and y. If i acts at a later stage, we want to destroy this factorization. To do this, we make y a unit.

We then introduce another factorization $p_i = x'y'$ for new x' and y', and continue, destroying it if i acts again.

Ring Theoretic Operations

In the above sketch, we start with $\mathbb{Z}$, and repeatedly expand it through the following two operations:

- Localization: This process embeds an integral domain into a larger one making some prescribed elements units.
- Introduce a Factorization: This consists of adjoining elements x and y and then introducing a relation $xy - p_i$, i.e. taking a quotient.

Ideally, we hope that these operations preserve nice algebraic properties of the ring, and do not disturb individual elements in significant ways.

Preserving Structure

Questions:

- Do these operations preserve important algebraic structure?
- Does introducing a new factorization for p_i destroy other primes? Does it introduce new units?
- Does making y a unit destroy other primes? Return the corresponding p_i to being prime (how do we know there aren't other factorizations)? Turn distinct primes into associates?
- What happens in the limit?

Adjoining an Element: Gauss and Hilbert

Theorem (Gauss)

If A is a UFD, then $A[x]$ is a UFD.

Theorem (Hilbert Basis Theorem)

If A is Noetherian, then $A[x]$ is Noetherian.

Corollary

If A is a Noetherian UFD, then $A[x]$ is a Noetherian UFD, as is $A[x, y]$, $A[x, y, z]$, $\ldots$.

Making Something a Unit

Recall that products of units are units, and divisors of units are units.

In $\mathbb{Z}[\sqrt{-14}]$, we have

$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$$

Each factor is irreducible, but none of the irreducibles are associates. If we turn 3 into a unit, then we automatically turn both $5 + 2\sqrt{-14}$ and $5 - 2\sqrt{-14}$ into units.

Localization

Let A be an integral domain and let S be a multiplicatively closed subset of A. There is an integral domain $S^{-1}A$, called the localization of A at S, with the following properties:

- A embeds into $S^{-1}A$ in such a way that every element of S is a unit in $S^{-1}A$.
- $S^{-1}A$ is the smallest integral domain with this property.

One can construct $S^{-1}A$ as the set of pairs (a, s) modulo the equivalence relation $(a, s) \sim (b, t)$ if $ta = sb$. Addition and multiplication behave as for fractions.

Localization Preserves Structure

Proposition

A localization of a UFD is a UFD.

Proposition

A localization of a Noetherian ring is Noetherian.

Corollary

A localization of a Noetherian UFD is a Noetherian UFD.

Turning a Prime into a Unit

Let A be a UFD and let $q \in A$ be prime. Let $S = \{1, q, q^2, \dots\}$, and consider the integral domain $B = S^{-1}A$.

Proposition

- *If A is a computable and $\{a \in A : q \mid a\}$ is computable, then we can build B as a computable extension of A.*
- *If $p \in A$ is prime and is not an associate of q in A, then p is prime in B.*
- *If $p_1, p_2 \in A$ are primes that are not associates in A, then they are not associates in B.*
- *If $p \in A$ is prime and $\{a \in A : p \mid a\}$ is computable, then $\{b \in S^{-1}A : p \mid b\}$ is computable (uniformly from an index).*

Quotients

Unfortunately, quotients destroy many algebraic properties. For example:

$$\mathbb{Z}[x]/\langle x^2 + 5 \rangle \cong \mathbb{Z}[\sqrt{-5}]$$

is a quotient of a UFD, but is not itself a UFD. Furthermore, in this quotient, 2 remains irreducible but we have destroyed the property of primeness.

We've also seen that quotients can introduce many unexpected units, as in:

$$\mathbb{Z}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Z}[\sqrt{2}]$$

Introducing a Factorization

Let A be a Noetherian UFD and let $q \in A$ be prime. Let

$$B = A[x, y]/\langle xy - q \rangle$$

Elements of B can be represented uniquely in the form

$$a_m x^m + \cdots + a_1 x + c + b_1 y + \cdots + b_n y^n$$

where the coefficients are from A and we multiply using the relation $xy = q$.

Introducing a Factorization

Proposition

- *If A is a computable, then we can build B as a computable extension of A.*
- *B is an integral domain.*
- *If $\sigma, \tau \in B$ and $\sigma\tau \in A$, then either both are in A, one is 0, or one is ax^n while the other is by^n.*

Corollary

- *$U(B) = U(A)$.*
- *If $p_1, p_2 \in A$ are primes that are not associates in A, then they are not associates in B.*
- *x and y are not associates in B.*
- *Neither x nor y is an associate of any element in A.*

Introducing a Factorization

Theorem

- *If $p \in A$ is prime and is not an associate of q in A, then p is prime in B.*
- *x and y are primes in B.*

Proposition

- *If $p \in A$ is prime and $\{a \in A : p \mid a\}$ is computable, then $\{\sigma \in B : p \mid \sigma\}$ is computable (uniformly from an index).*
- *If $\{a \in A : q \mid a\}$ is computable, then the sets $\{b \in B : x \mid \sigma\}$ and $\{b \in B : y \mid \sigma\}$ are computable (again uniformly).*

Proving UFD

Recall that $B = A[x, y]/\langle xy - q\rangle$. Working with B directly is difficult, but we can understand it more easily if we invert an element. Let S be the multiplicative set generated by x. We prove that $S^{-1}B$ is a UFD.

Theorem (Nagata's Criterion)

Let B be a Noetherian integral domain. Let Γ be a set of prime elements of B, and let S be the multiplicative set generated by Γ. If $S^{-1}B$ is a UFD, then so is B.

Proving UFD

Theorem

B is a Noetherian UFD.

Proof Sketch.

Elements of B look like A-linear combinations of powers of x and powers of y. Localization commutes with quotients, so inverting x is the same as inverting x in $A[x, y]$ and then taking the quotient. Now once we invert x we have $\langle xy - q \rangle = \langle y - \frac{q}{x} \rangle$, so essentially we are just inverting x in $A[x]$. But this is a localization of a UFD, hence a UFD. □

Construction

To work for i, we assume finite action, and introduce a new factorization $p_i = xy$ for new elements x and y. If i acts at a later stage, we want to destroy this factorization. To do this, we make y a unit, thus making p_i and x associates. Since x will remain prime in the extension, p_i will return to being prime. We then introduce a new factorization for p_i.

In this way, we build a sequence of Noetherian UFDs

$$\mathbb{Z} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$$

where we introduce factorizations and destroy them in response to our Π^0_2 set. Let $A_\infty = \bigcup_{n \in \omega} A_n$.

The Limit

Proposition

Let $a \in A_\infty$, so $a \in A_m$ for some m. The following are equivalent:

1. $a \in U(A_\infty)$.
2. $a \in U(A_n)$ *for all sufficiently large* $n \geq m$.
3. $a \in U(A_n)$ *for some* $n \geq m$.

Proposition

Let $p \in A_\infty$, so $p \in A_m$ for some m. If there are infinitely many $n \geq m$ such that p is prime in A_n, then p is prime in A_∞.

Corollary

p_i is prime in A_∞ if and only if $i \in Q$.

The Limit

Theorem

A_∞ is a UFD.

In general, the union of an ω-sequence of UFDs is not a UFD. However, the preservation of primes together with the previous corollary allow this to go through.