ABSTRACT ALGEBRA II
FACTORIZATION

MARIO L. GUTIERREZ ABED

Unique Factorization Domains

Definition. *Two elements $a, b \in \mathcal{R}$ are said to be* ***associates*** *in $\mathcal{R}$ if $a = bu$, where u is a unit in $\mathcal{R}$.* ★

Example: The only units in $\mathbb{Z}$ are 1 and -1. Thus the only associates of 26 in $\mathbb{Z}$ are 26 and -26. ▲

Definition. *A nonzero element p that is not a unit of an integral domain D is said to be an* ***irreducible*** *of D if in every factorization $p = ab$ in D, p has the property that either a or b is a unit.* ★

Remark: Note that an associate of an irreducible p is again an irreducible, for if $p = uc$ for a unit u, then any factorization of c provides a factorization of p.

Definition. *An integral domain D is said to be a* ***unique factorization domain*** *(abbreviated* UFD*) if the following two conditions are satisfied:*

- *Every element of D that is neither 0 nor a unit, can be factored into a product of a finite number of irreducibles.*
- *If $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates.* ★

Example: Theorem 23.20[1] shows that for a field F, we have that $F[x]$ is a UFD. Also we know that $\mathbb{Z}$ is a UFD:

For example, in $\mathbb{Z}$ we have

$$24 = (2)(2)(3)(2) = (-2)(-3)(2)(2).$$

Here 2 and -2 are associates, as are 3 and -3. Thus, except for order and associates, the irreducible factors in these two factorizations of 24 are the same. ▲

[1]Here's *Theorem 23.20*, for reference:
Theorem 23.20) If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique expect for order and for unit (that is, nonzero constant) in F.

Lemma. *Let D be a principal ideal domain* (PID)*. If $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \dots$ is an ascending chain of ideals $\mathcal{I}_i$, then there exists a positive integer r such that $\mathcal{I}_r = \mathcal{I}_s$ for all $s \geq r$. Equivalently, every strict ascending chain of ideals (all inclusions proper) in a* PID *is of finite length. We express this by saying that the **ascending chain condition** holds for ideals in a* PID*.*

Theorem. *Let D be a* PID*. Every element that is neither 0 nor a unit in D is a product of irreducibles.*

Lemma. *An ideal $\langle p \rangle$ in a* PID *is maximal if and only if p is irreducible.*

Lemma. *In a* PID*, if an irreducible p divides ab, then either $p \mid a$ or $p \mid b$.*

Corollary. *In a* PID*, if an irreducible p divides $a_1 a_2 \dots a_n$ for $a_i \in D$, then $p \mid a_i$ for at least one i.*

Definition. *A nonzero nonunit element p of an integral domain D is a **prime** if, for all $a, b \in D$, $p \mid ab$ implies either $p \mid a$ or $p \mid b$.* ★

Remark: It can be shown that a prime in an integral domain is always an irreducible and that in a UFD an irreducible is also a prime. Thus the concepts of primes and irreducibles coincide in a UFD. However, as the next example shows, these two concepts do not coincide in every domain. We show an integral domain containing some irreducibles that are not prime:

Example: Let F be a field and let D be the subdomain $F[x^3, xy, y^3]$ of $F[x, y]$. Then x^3, xy, and y^3 are irreducibles in D, but

$$(x^3)(y^3) = (xy)(xy)(xy).$$

Since xy divides x^3y^3 but not x^3 or y^3, we see that xy is not a prime. Similar arguments show that neither x^3 nor y^3 is a prime. ▲

Theorem. *Every* PID *is a* UFD*. (The converse is not true)*

Remark: Note that it follows at once that $\mathbb{Z}$ is a UFD, since it is a PID.

Definition. *Let D be a* UFD*. A nonconstant polynomial*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

*in $D[x]$ is said to be **primitive** if 1 is the* gcd *of the a_i, for $i = 0, 1, \dots, n$.* ★

Lemma. *If D is a* UFD*, then for every nonconstant $f(x) \in D[x]$ we have $f(x) = c \cdot g(x)$, where $c \in D$, $g(x) \in D[x]$, and $g(x)$ is primitive. The element c is unique up to a unit factor in D and it is known as the **content** of $f(x)$. Also, $g(x)$ is unique up to a unit factor in D.*

Lemma (**Gauss's Lemma**)**.** *If D is a* UFD*, then a product of two primitive polynomials in $D[x]$ is again primitive. (This lemma also applies for any finite product of primitive polynomials by applying induction.)*

Lemma. *Let D be a* UFD *and let F be a field of quotients of D. Let $f(x) \in D[x]$, where* $\deg(f(x)) > 0$*. If $f(x)$ is an irreducible in $D[x]$, then it is also an irreducible in $F[x]$. In addition, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.*

Remark: The preceding lemma shows that if D is a UFD, then the irreducibles in $D[x]$ are precisely the irreducibles in D, together with the nonconstant primitive polynomials that are irreducible in $F[x]$, where F is a field of quotients of D.

Corollary. *If D is a* UFD *and F is a field of quotients of D, then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees r and s in $F[x]$ if and only if it has a factorization into polynomials of the same degrees r and s in $D[x]$.*

Here's the main theorem of this subsection:

Theorem. *If D is a* UFD*, then $D[x]$ is also a* UFD*.*

Proof. See proof on Page $398 - 399$, *Fraleigh's.* □

Corollary. *If F is a field and $x_1, \ldots, x_n$ are indeterminates, then $F[x_1, \ldots, x_n]$ is a* UFD*.*

Example: Let F be a field and let x and y be indeterminates. Then by the preceding corollary, $F[x, y]$ is a UFD. Now consider the set N of all polynomials in x and y in $F[x, y]$ having constant term 0. Then N is an ideal, but not a principal ideal. Thus $F[x, y]$ is not a PID. ▲

Euclidean Domains

Definition. *A* ***Euclidean norm*** *on an integral domain D is a function ν mapping the nonzero elements of D into the nonnegative integers such that the following two conditions are satisfied:*

- *For all $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$, where we have that either $r = 0$ or $\nu(r) < \nu(b)$.*
- *For all $a, b \in D$, where neither a nor b is 0, we have $\nu(a) \leq \nu(ab)$.*

An integral domain D is said to be a ***Euclidean domain*** *if there exists a Euclidean norm on D.* ★

Example: The integral domain $\mathbb{Z}$ is a Euclidean domain, for the function $\nu(n) = |n|$ for $n \neq 0$ in $\mathbb{Z}$ is a Euclidean norm on $\mathbb{Z}$. The first condition holds by the division algorithm for $\mathbb{Z}$. The second condition follows from $|ab| = |a||b|$ and $|a| \geq 1$ for $a \neq 0$ in $\mathbb{Z}$. ▲

Example: If F is a field, then it follows that $F[x]$ is a Euclidean domain. To see why, notice that the function ν defined by $\nu(f(x)) = \deg(f(x))$ for $f(x) \in F[x]$, and $f(x) \neq 0$, is a Euclidean norm. The first condition follows by the division algorithm in $F[x]$, while the second condition holds since the degree of the product of two polynomials is the sum of their degrees. ▲

Theorem. *Every Euclidean domain is a* PID *(and hence a* UFD*).*

Theorem (Euclidean Algorithm). *Let D be a Euclidean domain with Euclidean norm ν, and let a and b be nonzero elements of D. Let r_1 be as in the first condition for a Euclidean norm, that is,*

$$a = bq_1 + r_1,$$

where either $r_1 = 0$ or $\nu(r_1) < \nu(b)$. If $r_1 \neq 0$, let r_2 be such that

$$b = r_1 q_2 + r_2,$$

where either $r_2 = 0$ or $\nu(r_2) < \nu(r_1)$. In general, let r_{i+1} be such that

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

where either $r_{i+1} = 0$ or $\nu(r_{r+1}) < \nu(r_i)$. Then the sequence $r_1, r_2, \ldots$ must terminate with some $r_s = 0$. If $r_1 = 0$, then b is a gcd *of a and b. If $r_1 \neq 0$ and r_s is the first $r_i = 0$, then a* gcd *of a and b is r_{s-1}.*

Furthermore, if d is a gcd *of a and b, then there exist λ and μ in D such that $d = \lambda a + \mu b$.*

Proof. See proof on Page 404 – 405, *Fraleigh's.* □

46.10 Example Let us illustrate the Euclidean algorithm for the Euclidean norm | | on $\mathbb{Z}$ by computing a gcd of 22,471 and 3,266. We just apply the division algorithm over and over again, and the last nonzero remainder is a gcd. We label the numbers obtained as in Theorem 46.9 to further illustrate the statement and proof of the theorem. The computations are easily checked.

$$\begin{array}{rl}
 & a = 22{,}471 \\
 & b = 3{,}266 \\
22{,}471 = (3{,}266)6 + 2{,}875 & r_1 = 2{,}875 \\
3{,}266 = (2{,}875)1 + 391 & r_2 = 391 \\
2{,}875 = (391)7 + 138 & r_3 = 138 \\
391 = (138)2 + 115 & r_4 = 115 \\
138 = (115)1 + 23 & r_5 = 23 \\
115 = (23)5 + 0 & r_6 = 0
\end{array}$$

Thus $r_5 = 23$ is a gcd of 22,471 and 3,266. We found a gcd without factoring! This is important, for sometimes it is very difficult to find a factorization of an integer into primes. ▲

46.11 Example Note that the division algorithm Condition 1 in the definition of a Euclidean norm says nothing about r being "positive." In computing a gcd in $\mathbb{Z}$ by the Euclidean algorithm for $|\ |$, as in Example 46.10, it is surely to our interest to make $|r_i|$ as small as possible in each division. Thus, repeating Example 46.10, it would be more efficient to write

$$\begin{array}{rl} & a = 22{,}471 \\ & b = 3{,}266 \\ 22{,}471 = (3{,}266)7 - 391 & r_1 = -391 \\ 3{,}266 = (391)8 + 138 & r_2 = 138 \\ 391 = (138)3 - 23 & r_3 = -23 \\ 138 = (23)6 + 0 & r_4 = 0 \end{array}$$

We can change the sign of r_i from negative to positive when we wish since the divisors of r_i and $-r_i$ are the same. ▲