Part IX (§45- 47)
Factorization

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

45 Unique Factorization Domain (UFD)

Abstract

We prove evey PID is an UFD. We also prove if D is a UFD, then so is $D[x]$.

Definition 45.1. *Suppose R is a commutative ring (as always with unity 1).*

1. *Let $a, b \in R$. If $b = ac$ for some $c \in R$, we say that a* **divides** *b.* In this case, we write $a|b$.
2. *An element $u \in R$ is called an* **unit** *in R, if it has an inverse in R.* This is same as saying $a|1$.
3. *Two elements $a, b \in R$ would be called* **associatates**, *if $a = ub$ for some unit $u \in R$.* (Note, being associates is an equivalence relation.)

4. *Assume R is an integral domain. An nonunit $p \in R$ is said to be and* **irreducible** *element, if*

$$p = ab \quad \Longrightarrow \quad a \quad \text{or} \quad b \quad \text{is a unit.}$$

Note, if p is irreducible and $q = ub$ for some unit $u \in R$, then q is also irreducible. In other words, if p, q are associtesthen p is irreducible if and only if q is irreducible.

Now, we define Unique Factorization domain.

Definition 45.2. *Suppose D is an integral domain. We day D is an* **Unique Factorization domain (UFD)**, *if*

1. *Each nonzero, nonunit element $a \in D$ is a product of irreducible elemnets.*
2. **(Uniqueness):** *For such a nonzero, nonunit element $a \in D$, if*

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad \text{where} \quad p_i, q_j \quad \text{are irreducible}$$

then $r = s$ and q_j can be relabeled so that p_i, q_i are associates.

Example 45.3. 1. The ring of integers $\mathbb{Z}$ is a UFD.

2. If F is a field, then the polynomial ring $F[x]$ is a UFD (see theorem 23.20).

We also define principal ideal domain (PID).

Definition 45.4. *An integral domain D is said to be a* **principal ideal domain (PID)**, *if every ideal is principal* (i.e. any ideal $I = Dx$ for some x.)

The goal of this section is prove two theorems:

1. Every PID is a UFD,
2. If D is a UFD, so is the polynomial ring $D[x]$.

45.1 Every PID is a UFD

Lemma 45.5. Let R be a commutative ring and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \quad \textit{is an ascending chain of ideals of} \quad R.$$

Then $I = \cup_{i=1}^{\infty} I_i$ is an ideal.

Proof. Let $a, b \in I$. Then, $a \in I_i$ and $b \in I_j$ for some i, j. We can assume $i \leq j$, and hence $a, b \in I_j$. So, $a \pm b \in I_j$, hence $a \pm b \in I$.

Also, if $a \in I$ and $c \in R$, we would like to prove $ca \in I$. First, $a \in I_i$ for some i. So, $ca \in I_i$. So, $ca \in I$.

The proof is complete. ■

Lemma 45.6. *Let D be a PID. Let*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \quad \textit{is an ascending chain of ideals of} \quad D.$$

Then, there is an integer n such that $I_i = I_n$ for all $i \geq n$. (We say every ascending chain of ideals terminates. We also say that ascending chain condition (ACC) holds for ideals in D.)

Proof. First, $I = \cup_{i=1}^{\infty} I_i$ is an ideal. Since D is a PID, $I = Da$ for some $a \in I$. So, there is an integer n such that $a \in I_n$. So, $I = Da \subseteq I_n$. So, $I_n = I$. Therefore,

$$I_n = I \subseteq I_r \subseteq I \quad \forall \quad r \geq n. \quad So, I_n = I = I_r \quad \forall \quad r \geq n.$$

The proof is complete. ■

Remark. Any ring R that satisfies ACC for ideals is called a Noetherian ring. Noetherian rings are the main focus of higher level algebra courses at KU.

Lemma 45.7. *Let D be an integral domain.*

1. *For elements $a, b \in D$,*

$$Da \subseteq Bb \qquad \Longleftrightarrow \qquad b|a.$$

2. For elements $a, b \in D$,

$$Da = Db \qquad \Longleftrightarrow \qquad a, b \quad \textit{are associates.}$$

Proof. (1) is obvious. For (2), $Da = Db$. Since $a \in Db$, we have $a = \lambda b$ for some $\lambda \in D$. Similarly, $b = \mu a$ for some $\mu \in D$. So,

$$a = \lambda b = \lambda \mu a. \quad \textit{So}, \quad \lambda \mu = 1.$$

So, λ is an unit. Therefore, a, b are associates. The proof is complete.■

Remark. A lot of properties we studied about the polynomial rings $F[x]$ are also enjoyed by any PID, as follows.

Theorem 45.8 (45.11)**.** *Let D be a PID. For $a \in D$, if $a \neq 0$ and not a unit, then a is product of irreducible elements in D.*

Proof.
Claim: a has an irreducible factor.

If a is irreducible then the claim is established. If a is not irreducible, $a = a_1 b_1$, for some nonzero nonunits a_1, b_1. If one of them is irreducible, then the claim is established. So, assume both are reducible. So,

$$Da \subset Da_1 \quad \textit{and} \quad Da \neq Da_1.$$

Now we apply the same argument to a_1. Since a_1 is reducible, $a_1 = a_2 b_2$ for or some nonzero nonunits a_2, b_2. If one of them is irreducible, then the claim is established, because $a = b_1 a_2 b_2$. If both are reducible, this process continues an we have a chain

$$Da \subset Da_1 \subset Da_2 \cdots$$

Since ACC for ideals holds in D, this process must terminate. So, a_r is irreducible, and $a = b_1 b_2 \cdots b_{r-q} a_r$. So, the claim is established.

Now write $a = p_1 c_1$, where p_1 is irreducible. If c_1 is irreducible, then the proof is complete. If not $c_1 = p_2 c_2$, where p_2 is irreducible. This way we get a chain of ideals

$$Da \subset Dc_1 \subset Dc_2 \cdots$$

again, since ACC for ideals holds in D, this process must terminate. So, c_k irreducible, for some k and $a = p_1 p_2 \cdots p_{r-1} c_r$ is a product of irreducible factors. The proof is complete. ■

Lemma 45.9 (45.12)**.** *Let D be a PID and $p \in D$. Then, p is irreducible if and only if Dp is a maximal ideal.*

Proof. ($\Rightarrow$): Suppose p is irreducible. Since p is not a unit, $Dp \neq D$. If Dp is not maximal, then there is an ideal I such that $Dp \subset I$ and $Dp \neq I$. Since D is a PID $I = Da$ for some nonunit $a \in D$. Noe $p \in I = Da$. So, $p = ba$ for some b. Since $I \neq Dp$, b is also a nonunit. This contradicts that p is irreducible. This establishes that Dp is maximal.
($\Leftarrow$): Suppose Dp is maximal. Suppose $p = ab$. Assume a is not an unit. Then $Dp \subseteq Da$. Since Dp is maximal, $Dp = Da$. By the lemma above p, a are associates. So, p is irreducible. The proof is complete.■.

Theorem 45.10 (45.13)**.** *Suppose D is a PID and $p \in D$ is an irreducible element. Now, for $a, b \in D$ we have*

$$p|ab \qquad \Longrightarrow \qquad (p|a \quad or \quad p|b).$$

Proof. Since p is irreducible, Dp is maximal ideal. So, Dp is a prime ideal. Since $p|ab$ we have $ab = \lambda p \in Dp$. Since Dp is prime, either $a \in Dp$ or $b \in Dp$. Which is same as saying either $p|a$ or $p|b$. The proof is complete. ■

Corollary 45.11. *Suppose D is a PID and $p \in D$ is an irreducible element. For $a_i \in D$ we have*

$$p|a_1 a_2 \cdots a_n \qquad \Longrightarrow \qquad p|a_i \quad for\ some \quad i = 1, \ldots, n.$$

Proof. Use induction. The proof is complete. ■

Definition 45.12. *Let R be an integral domain. A nonzero nonunit $p \in R$ is called a* **prime element** *if for $a, b \in D$ we have*

$$p|ab \qquad \Longrightarrow \qquad (p|a \quad or \quad p|b).$$

Lemma 45.13. *Let D be a PID. Then,*

$$\text{an element } \; p \in D \; \text{ is irreducible } \iff \; p \; \text{ is prime.}$$

Proof. Suppose p is irreducible. Then, by theorem 45.10, p is prime.

Now suppose p is a prime. Suppose p is not reducible. So, $p = ab$. So, $p|a$ or $p|b$. Without loss of generality, assume $p|a$. So, $a = \lambda p$. So, $p = ab = \lambda pb$. So, $\lambda b = 1$. Hence, b is a unit. The proof is complete.■

Following theorem is analogous to theorem 23.20 on polynomial rings $F[x]$.

Theorem 45.14 (45.17)**.** *Suppose D is a PID. Then D is a UFD.*

Proof. By theorem 45.8, any nonzero element $a \in D$ is product of irreducible element.

The proof of the uniquenss of such factorization is exactly same as that of theorem 23.20. I leave it as an exercise. The proof is complete.■

Remark.

1. Suppose F is a field F.
   (a) We proved that the polynomial ring $F[x]$ is a PID.
   (b) We also proved $F[x]$ is a UFD, independently.
   The same follows from the above theorem.
   (c) However, polynomial ring $F[x, y]$ in two indeterminates is not a PID. The ideal $(x, y) := F[x, y]x + F[x, y]y$ is not principal.
2. The ring of integers $\mathbb{Z}$ is a PID and a UFD.

45.2 If D is a UFD, then so is $D[x]$

We start with the definition of gcd.

Definition 45.15. *Let D be a UFD and $a_1, a_2, \ldots, a_n \in D$. An element $d \in D$ is called a* **greatest common divisor (gcd**, *if*

1. *$d|a_i$ for all $i = 1, 2, \ldots, n$.*
2. *If there is another element $c \in D$ such that $c|a_i$ for all $i = 1, 2, \ldots, n$, then $c|d$.*

Usually, there are more than one gcds for any given $a_1, a_2, \ldots, a_n \in D$. However, if c, d are two gcds of $a_1, a_2, \ldots, a_n \in D$, then

$$c|d \quad and \quad d|c. \quad So, \quad c, d \quad are\ associates.$$

For integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ if $d = gcd(a_1, a_2, \ldots, a_n)$ then so is $-d$, according to this definition. At high school, the positive gcd is refered to as "the gcd".

45.3 Premitive Polynomial

In §23 discussed when a polynomial with integer coefficients is called primitive. We extend the same as follows.

Definition 45.16. *Suppose D is a UFD. A non constant polynomial*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$$

is called **premitive** *if*

$$gdc(a_0, a_1, \ldots, a_n) = 1.$$

Lemma 45.17 (45.22)**.** *Suppose D is a UFD and*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x] \quad be\ a\ polynomial.$$

Then

1. **Definition:** *$c = gcd(a_0, a_1, \ldots, a_n)$ is called the* **content of** *f. The content is unique only upto associates.*
2. *$f(x) = cg(x)$ where $g(x) \in D[x]$ is a primitive polynomial.*

Proof. Obvious. ■

The following is an analogue of a theorem (not in the textboo; but I did) in §23 on polynomials with integer coefficients.

Lemma 45.18 (45.25 Gauss Lemma)**.** *Suppose D is a UFD. Then the product of two premitive polynomial in $D[x]$ is primitive.*

Proof. (*It will exactly same as that in §23. I will copy and paste.*)

Write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{and} \quad g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

where $a_i, b_j \in D$. Suppose $p \in D$ is an irreducible element. We will show p does not divide some coefficient of $f(x)g(x)$. Since f is primitive p does not divide some coefficient of f. Let a_j be the first one:

$$p|a_0, p|a_1, \ldots, p|a_{j-1}, p \not| a_j.$$

Similarly, there is a k such that

$$p|b_0, p|b_1, \ldots, p|b_{k-1}, p \not| b_k.$$

Now, coefficient c_{j+k} of x^{j+k} in $f(x)g(x)$ is give by $c_{j+k} =$

$$a_j b_k + (a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \cdots + a_{j+k} b_0) + (a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \cdots + a_0 b_{j+k})$$

Now, $p \not| a_j b_k$ and all the other terms are divisible by p. So, $p \not| c_{j+k}$. The proof is complete. ■

Corollary 45.19. *Suppose D is a UFD. Then product of finitely many premitive polynomials in $D[x]$ is primitive.*

Proof. Use Induction. ■

Before we proceed, let me remind you again, for a field F, the polynomial ring $F[x]$ is a UFD (in fact a PID).

Lemma 45.20 (45.27)**.** *Let D be a UFD and F be the field of fractions of D. Let $f(x) \in D[x]$ be a nonconstant polynomial.*

1. *If $f(x)$ is irreducible in $D[x]$, then $f(x)$ is also irreducible in $F[x]$.*
2. *If $f(x)$ is premitive in $D[x]$ and is irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.*

Proof. To prove the first point, assume $f(x)$ is irreducible in $D[x]$. Now suppose

$$f(x) = r(x)s(x) \quad \textit{where } r(x), s(x) \in F[x]; \ \deg(r) < \deg(f), \ \deg(s) < \deg(f).$$

We do the process of "clearing denominators" as follows: Write

$$r(x) = \frac{a_0 + a_1x + a_2x^2 + \cdots + a_tx^t}{d_1} = \frac{r_1(x)}{d_1} = \frac{c_1r_2(x)}{d_1}$$

where $a_i, d_1 \in D$ and r_1 is the numerator, $c_1 = \mathit{content}(r_1)$ and r_2 is a primitive polynomial. Similarly,

$$s(x) = \frac{c_2s_2(x)}{d_2} \quad \textit{where } c_2, d_2 \in D, \quad s_2(x) \in D[x] \ \textit{ is primitive.}$$

Write $f(x) = cg(x)$, where $c = \mathit{content}(f)$ and g is primitive. So, we have

$$f(x) = cg(x) = r(x)s(x) = \frac{(c_1c_2)r_2(x)s_2(x)}{d_1d_2}$$

or

$$(cd_1d_2)g(x) = (c_1c_2)(r_2(x)s_2(x)).$$

Since $_2(x), s_2(x)$ are primitive, so is the product $r_2(x)s_2(x)$. Since the content of two sides must be associates,

$$c_1c_2 = ucd_1d_2 \qquad \textit{for some unit} \quad u \in D.$$

There fore

$$(cd_1d_2)g(x) = (ucd_1d_2)(r_2(x)s_2(x)). \qquad \textit{or} \quad f(x) = cg(x) = ucr_2(x)s_2(x).$$

So, we have shown that $f(x)$ is has a nontrivial factorization in $D[x]$, which contradicts the hypothesis. So, $f(x)$ is irreducible in $F[x]$. This completes the proof of (1).

Remark. *In fact, $f(x)$ factors in to polynomials of same degree in $D[x]$.*

To prove (2), assume that f is primitive and irreducible in $F[x]$. Let $f(x) = r(x)s(x)$ be non trivial factorization in $F[x]$. Since f is primitive, neither r nor s are constant (in fact both are premitive. This means $0 < \deg(r) < \deg(f), 0 < \deg(s) < \deg(f)$. So, $f(x)$ factors into two polynomials of degree less than $\deg(f)$ in $F[x]$, which is a contradiction. The proof is complete. ■

Corollary 45.21 (45.28)**.** *Suppose D is a UFD and F is the field of its fractions. Let $f(x) \in D[x]$ be a nonconstant polynomial. Suppose*

$$f(x) = r(x)s(x) \quad \textit{for some } r, s \in F[x] \textit{ with } \deg(r) < \deg(f), \deg(s) < \deg(f).$$

Then

$$f(x) = r_1(x)s_1(x) \quad \textit{for some } r_1, s_1 \in D[x] \textit{ with } \deg(r_1) = \deg(r), \deg(s_1) = \deg(s).$$

Proof. See the remark in the proof of 45.20. ■

Before we state our main theorem, I want to settle *Who are the irreducible elements in $D[x]$.*

Lemma 45.22 (Extra)**.** *Let D be a UFD.*

1. *Suppose $p \in D$ is irreducible in D. Then, p is irreducible in $D[x]$.*
2. *Let F be the field of fractions of D. Suppose $f(x) \in D[x]$ with $\deg(f) > 0$. Then, f is irreducible in $D[x]$ if and only if f is premitive and f is irreducible in $F[x]$.*

Proof. Suppose $p \in D$ is irreducible. If p has a nontrivial factorization in $D[x]$, by degree comparison, factor must be constants. So, that will give a nontrivial factorization of p in D. So, p is irreducible in $D[x]$.

To prove (2), first suppose f is irreducible in $D[x]$. Write $f(x) = cg(x)$ where $c = content(f) \in D$ and g is premitive. If c is nonunit, then $f(x) = cg(x)$ is a nontrivial factorization. So, c is a unit. This means f is premitive.

Now if $f(x)$ has a nontrivial factorization in $F[x]$, it factors into polynomials of smaller degree. By (45.21), then f will also factors into polynomials of smaller degree in $D[x]$. Which would contradicts the hypothesis. So, f is irreducible in $F[x]$.

Now, we prove the converse. Suppose f is premitive and f is irreducible in $F[x]$. Suppose $f(x) = r(x)s(x)$ be a nontrivial factorization of f in $D[x]$. Since f is premitive, $r(x), s(x)$ are nonconstant polynomials. So, $f(x) = r(x)s(x)$ is a nontrivial factorization of f in $F[x]$. This would be a contradicts the hypothesis. So, f is irreducible in $D[x]$.

The proof is complete. ■

Theorem 45.23 (45p29)**.** *Suppose D is a UFD. Then, the polynomial ring $D[x]$ is a UFD.*

Proof. (**Existance of factorization**): Suppose $f \in D[x]$ be nonunit. Write $f(x) = cg(x)$ where $c = content(f) \in D$ and g is a premitive polynomials. Since D is UFD

$$c = p_1 p_2 \cdots p_m$$

where $p_i \in D$ is irreducible in D and hence irreducible in $D[x]$.

Again, let F be the field of fractions of F. Since $F[x]$ is a UFD

$$g(x) = q_1(x)q_2(x) \cdots q_n(x)$$

where q_i are irreducible in $F[x]$. By (45.21),

$$g(x) = P_1(x)P_2(x) \cdots P_n(x) \qquad P_i \in D[x] \ \ and \ \ \deg(P_i) = \deg(q_i).$$

Since g is premitive, P_i are premitive. By uniqueness of factorization in $F[x]$, P_i, q_i are associates. So, P_i is irreducible in $F[x]$. By (45.22),

P_i are irreducible in $D[x]$. So,

$$f(x) = cg(x) = p_1 p_2 \cdots p_m P_1(x) P_2(x) \cdots P_n(x)$$

is a factorization of $f(x)$ in to irreducible elements in $D[x]$.
Uniqueness of Factorization: Let $f(x) = cg(x) \in D[x]$ where $c = content(f)$ and g is premitive. Suppose

$$f(x) = p_1 p_2 \cdots p_m P_1(x) P_2(x) \cdots P_n(x) = q_1 q_2 \cdots q_s Q_1(x) Q_2(x) \cdots Q_r(x)$$

where $p_i, q_i, \in D$ are irreducible and $P_i, Q_i \in D[x]$ are irreducible polynomials of positive degree.

Comparing contents

$$c = up_1 p_2 \cdots p_m = vq_1 q_2 \cdots q_s$$

for some units u, v. Since D is a UFD, after relabeling (and adjusting the units), we have $m = s$ and $p_i = q_i$.

So, we have

$$g(x) = P_1(x) P_2(x) \cdots P_n(x) = Q_1(x) Q_2(x) \cdots Q_r(x).$$

Since $g(x)$ is premitive, P_i, Q_i are premitive. So, P_i, Q_i are irreducible in $F[x]$. Since $F[X]$ is a UFD, $r = m$ and after relabeling, $P_i = \frac{a_i}{b_i} Q_i$, where $a_i, b_i \in D$. So, $b_i P_i = a_i Q_i$. Comparing contents, $b_i = u_i a_i$. So, $u_i a_i P_i = a_i Q_i$. or $u_i P_i = Q_i$. So, P_i, Q_i are associates.

The proof is complete. ■

Corollary 45.24 (45.30)**.** *Let F be a field and $x_1, \ldots, x_n$ be indeterminates. Then the polynomial ring $F[x_1, \ldots, x_n]$ is a UFD.*

Proof. Inductively, $F[x_1, \ldots, x_r] = F[x_1, \ldots, x_{r-1}][x_r]$ is a UFD, by thoerem 45.23.

Exercise 45.25. *Let F be a field and $R = F[x, y]$ be the polynomial ring. Prove that the ideal $(x, y) := Rx + Ry$ is not principal.*

46 Euclidain Domain

Intuitively, a Euclidian Domain is a commutative ring where Division Algorithm works. We prove any Euclidian Domain is a PID.

Definition 46.1 (46.1)**.** *A* **Euclidian norm** *on an integral domain D is a function*

$$\nu : D \setminus \{0\} \longrightarrow \{0, 1, 2, 3, \ldots\}$$

such that

1. *For $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that*

$$a = bq + r \quad \textit{where} \quad r = 0 \quad \textit{or} \quad \nu(r) < \nu(b).$$

2. *For $a, b \in D$, where $a \neq 0, b \neq 0$, we have*

$$\nu(a) \leq \nu(ab).$$

An integral domain with an Euclidian norm is called a **Euclidian domain**.

Example 46.2.

1. For $n \in \mathbb{Z}$ and $n \neq 0$ define $\nu(n) = |n|$. Then, ν is an Euclidian norm on $\mathbb{Z}$. So, $\mathbb{Z}$ is an Euclidian domain.
2. Let F be a field and $F[x]$ be the polynomial ring. For $f \in F[x]$ and $f \neq 0$ define $\nu(n) = \deg(f)$. Then, ν is an Euclidian norm on $F[x]$. So, $F[x]$ is an Euclidian domain.

Theorem 46.3 (46.4)**.** *Every Euclidean domain D is a PID.*

Proof. Let D be an Euclidean domain with Euclidean norm ν. Let I is an ideal. We will prove that I is principal. If $I = \{0\}$, then it is principal. So, assume I has nonzero elements. Let

$$n = \min\{\nu(x) : x \in I, x \neq 0\}.$$

Let $b \in I$ be such that $\nu(b) = n$. We will prove $I = Db$ (*We follow the same argument we used for polynomial rings.*)

Since $b \in D$, we have $Rb \subseteq I$. Now, let $a \in I$.

$$a = bq + r \quad where \quad r = 0 \quad or \quad \nu(r) < \nu(b).$$

But $r = a - bq \in I$. So, by minimality of $\nu(b)$, we have $r = 0$. So, $a = bq \in Db$. So, $I = Db$. The proof is complete. ■

Corollary 46.4. *Every Euclidean domain D is a UFD.*

Proof. By above theorem O is a PID, hence a UFD. ■

46.1 Units in Euclidean Domains

Theorem 46.5 (46.6)**.** *Let D be an Euclidean domain with Euclidean norm ν.*

1. *Then,*
$$\nu(1) = \min\{\nu(x) : x \in D, x \neq 0\}.$$
2. *For $u \in D$ we have*
$$u \quad is\ a\ unit \Longleftrightarrow \nu(u) = \nu(1).$$

Proof. (1) follows from the second property of nu as follows:

$$\forall\ a \in D, a \neq 0 \qquad \nu(1) \leq \nu(1a) = \nu(a).$$

To prove (2) suppose $u \in D$ is a unit. Then,

$$\nu(1) \leq \nu(u) \leq \nu(uu^{-1}) = \nu(1). \qquad So \quad \nu(u) = \nu(1).$$

Conversely, suppose $\nu(1) = \nu(u)$. Se divide ! by u, we have

$$1 = uq + r \qquad for\ some\ \ q, r \in D \quad \ni \quad r = 0\ \ or\ \ \nu(r) < \nu(u).$$

Since $\nu(u) = \nu(1)$ is minimum, $r = 0$. So, $1 = uq$. So, u is a unit. The proof is complete. ■

Theorem 46.6 (46.9)**.** *(***Euclidean Algorithm***): Suppose D is an Euclidean domain. Then the Euclidean Algorithm of computing gcd(a, b) by long division works.*

Proof. Exercise/skip.

47 Gaussian Integers

Definition 47.1. A complex numbers $a + bi$ with $a, b \in \mathbb{Z}$ is called a **Gaussian Integer**.

1. The set $\mathbb{Z} + \mathbb{Z}i$ of all Gaussian Integers forms anintegral domain.

2. For $x = a + bi \in \mathbb{Z} + \mathbb{Z}i$ define

$$N(x) = a^2 + b^2.$$

   This function N will be called a/the **norm** on $\mathbb{Z} + \mathbb{Z}i$. N has the following properties: For $x, y \in \mathbb{Z} + \mathbb{Z}i$

   (a) $N(x) \geq 0$

   (b)
$$n(x) = 0 \qquad \Longleftrightarrow \qquad x = 0$$

   (c)
$$N(xy) = N(x)N(y).$$

3.

   Theorem 47.2 (47.4)**.** *N is an Euclidean norm.*

   Proof. skip.