Chapter 5

Factorization

02/17/2016

Thoughtout this chapter, D stands for an integral domain, unless indicated otherwise.

The most important theorem in this course, after the Fundamental Theorem of Galois Theory, can be briefly stated as follows.

Theorem 5.0.1 *Field* $\Rightarrow$*ED* $\Rightarrow$*PID* $\Rightarrow$*UFD* $\Rightarrow$*ID*

In other words, every field is an Euclidian Domain; every Euclidean Domain is a Principal Ideal Domain; every Principal Ideal Domain is a Unique Factorization Domain; and every Unique Factorization Domain is an Integral Domain. So far, we only have the definition for the first and last of these expressions. In the next few days, we will give the appropriate definitions of the other terms, prove each of the implications, and show, by counterexample, that all implications are strict.

5.1

Definition 5.1.1. An Euclidean Domain consists of an integral domain D and a function $\delta : D - \{0\} \to \mathbb{N}$, satisfying the following condition:

For any $f, g \in D$ with $g \neq 0$, there exist $q, r \in D$ s.t.

$$f = gq + r \quad \text{and,} \quad \text{either} \quad r = 0, \quad \text{or} \quad \delta(r) < \delta(g).$$

The function δ is refered to as *divisiion function*, or *measure*, or *degree*.

Examples 5.1.1. 1. $\mathbb{Z}$ with $\delta(n) = |n|$.

2. For a field F, the ring $F[x]$ of polynomials over F with $\delta(f) = \deg(f)$.
3. $\mathbb{Z}(i)$ the ring of Gaussian integers with $\delta(m + ni) = m^2 + n^2 = N(m + ni)$.

Proposition 5.1.1 *If F is a field, then it is an Euclidean Domain, with $\delta(a) = 1$ for all $a \neq 0$.*

Note that the function δ is never used here, since the residue is always 0. In other words, a field has *exact* division.

Definition 5.1.2. A *Principal Ideal Domain* (PID) is an integral domain in which every ideal is principal, i.e. generated by a single element.

Example 5.1.2. $\mathbb{Z}$ is an PID.

We get more examples of PIDs from the following proposition.

Proposition 5.1.2 *If D is an Euclidean Doamin, then it is a PID.*

Proof. Let $I \trianglelefteq D$. If $I = \{0\}$ then $I = \langle 0 \rangle$.
Assume $I \neq \{0\}$. Let $0 \neq a \in I$, such that $\delta(a)$ is smallest among non-zero elements of I.
Claim: $I = \langle a \rangle$. Clearly $\langle a \rangle \subseteq I$. Let $b \in I$. Since D is an ED there exist $q, r \in D$ such that

$$b = aq + r \quad \text{and,} \quad \text{either } r = 0, \quad \text{or} \quad \delta(r) < \delta(a).$$

Since $a, b \in I$, we that $r = b - aq \in I$. Minimality of $\delta(a)$ force $r = 0$, so $b = aq \in \langle a \rangle$. ∎

We get from this proposition and Examples 5.1.1 that in addition to $\mathbb{Z}$, the ring $\mathbb{Z}(i)$ of Gaussian integers is a PID, and for any field F, the ring $F[x]$ of polynomials over F is also a PID.

Definition 5.1.3. Let $a, b \in D$. We say that a *divides* b if there is $c \in D$ such that $b = ac$, i.e. $b \in \langle a \rangle$. We may also say that a is a *divisor* of b, or that b is a *multiple* of a.

02/18/16

Remark 5.1.1. Let $a, b, b_1, b_2, r \in D$.

1. $a|a$
2. $a|0$
3. $1|a$
4. $a|b_1, a|b_2 \Rightarrow a|(b_1 + b_2)$
5. $a|b \Rightarrow a|rb$

Definition 5.1.4. a, b are said to be *associates* in D if $a|b$ and $b|a$. We write $a \sim b$.

Proposition 5.1.3 *Let $a, b \in D$. TFAE*

1. *a, b are associates in D*
2. *there is a unit $u \in D^*$ such that $a = ub$*
3. *$\langle a \rangle = \langle b \rangle$*

Proof. (1) $\Rightarrow$(2) $\Rightarrow$(3) $\Rightarrow$(1) ■

Recall that for $p \in \mathbb{Z}$, not zero, not ± 1, TFAE:

1. $p = ab \Rightarrow a = \pm 1$ or $b = \pm 1$.
2. $p|ab \Rightarrow p|a$ or $p|b$, i.e. $ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$.

We extend these two ideas to an arbitrary ID D. In general they are not equivalent, like they are in $\mathbb{Z}$. We have an example of that in Examples 5.1.3 below.

Definition 5.1.5. Let $p \in D$ be a non-zero non-unit element (*nznu* for short). `irreducible` `prime`

1. We say p is *irreducible* if
$$p = ab \Rightarrow a \quad is\ a\ unit, or \quad b \quad is\ a\ unit.$$
2. We say p is *prime* if
$$p|ab \Rightarrow p|a \text{ or } p|b, \quad \text{i.e.} \quad ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle \text{ or } b \in \langle p \rangle.$$

Note that the condition for *irreducible* is equivalent to
$$p = ab \Rightarrow p \sim a \text{ or } p \sim b.$$
The condition for p is *prime* is equivalent to $\langle p \rangle$ is a prime ideal.

Proposition 5.1.4 *Let $p \in D$ be nznu.*

1. *If p is prime then p is irrreducible.*
2. *Assume D is a PID. If p is irreducible then p is prime.*

Proof. 1. Assume p is prime. WTS p is irreducible. Suppose $p = ab$. Then $p|ab$ and by primality $p|a$ or $p|b$. WLOG $p|a$, so $a = pc$ for some $c \in D$, and $p = ab = pcb$. Since D is an ID, and $p \neq 0$ we get $1 = cb$, so b is a unit.

2. Assume now that D is a PID and p is irreducible. WTS p is prime. Suppose $p|ab$, where $a, b \in D$. Let
$$I = \{xa + yp | x, y \in D\} = \langle a \rangle + \langle p \rangle \trianglelefteq D$$
Since D ia PID, there is $d \in D$ such that $I = \langle d \rangle$. Now we have $p \in I$ so there is $z \in D$ such that $p = zd$. Since p is irreducible, either d is a unit or $p \sim d$. If d is a unit then $I = D$, and $1 \in D$, so there are $x, y \in D$ such that $1 = xa + yp$. We get $b = xab + ypb$, and since $p|ab$, we get $p|b$. On the other hand, if $p \sim d$ then $\langle p \rangle = \langle d \rangle = I$, and since $a \in I$ we get $p|a$.

■

Examples 5.1.3. 1. $1 + i \in \mathbb{Z}(i)$ is irreducible, hence it is prime. Use that fact the $N(1+i) = 2$ and the norm N is a multiplicative function.

Unique Factorization Domain

2. $1 + \sqrt{-5} \in \mathbb{Z}(\sqrt{-5})$ is irreducible, and so is $1 - \sqrt{-5}$. Use the fact that $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, but there are no elements in $\mathbb{Z}(\sqrt{-5})$ with norm equal to 2 or 3. However, $1 + \sqrt{-5}$ is not a prime since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$ but $N(2) = 4$, $N(3) = 9$, and therefore $1 + \sqrt{-5}$ cannot divide either 2 or 3. From Proposition 5.1.4 we conclude that $\mathbb{Z}(\sqrt{-5})$ is not a PID. A similar argument shows that 2 and 3 are irreducible but not prime in $\mathbb{Z}(\sqrt{-5})$. It also shows that $\mathbb{Z}(\sqrt{-5})$ is not a UFD, see Definition 5.1.6 below.

Definition 5.1.6. An integral domain D is called a *Unique Factorization Domain* (UFD), if every nznu $a \in D$ can be factored as a product of irreducible elements, in a unique way up to order and associates. The uniqueness means that if

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

with all the p_is and q_js irreducible, then $r = s$, and, after some possible reordering, we get $p_i \sim q_i$ for $i = 1, \ldots, r$.

By definition, every UFD is an integral domain, so we get for free the implication UFD $\Rightarrow$ID in Theorem 5.0.1. In showing that an integral domain D is a UFD, we usually break the argument into two parts. For any nznu $a \in D$,

Existence: there exists a factorization of a into irreducible factors;

Uniqueness: two such factorizations have the same number of factors, and differ only on the order of the factors, and up to associates.

Examples 5.1.4. 1. Since in $\mathbb{Z}$ primes and irreducible are the same, the Fundamental Theorem of Arithmetic tells us that $\mathbb{Z}$ is a UFD.

2. Example 5.1.3 above, show that $\mathbb{Z}(\sqrt{-5})$ is not a UFD. This shows that the implication UFD $\Rightarrow$ID in Theorem **??** is strict.

3. For a field F, the ring $F[x]$ is a UFD. This follows from Proposition 5.1.8 below, together with Proposition 5.1.2 and the fact that $F[x]$ is an ED.

02/19/16

Ascending Chain Condition
Noetherian

Definition 5.1.7. We say that a ring R satisfies the *Ascending Chain Condition* (ACC), if every ascending chain of ideals

$$I_1 \leq I_2 \leq \cdots$$

has to become constant after a finite number of steps. That is, there is $n \geq 1$, such that $I_n = I_{n+1} = \cdots$. A ring that satisfies the ACC is called *Noetherian*.

Proposition 5.1.5 ?? *Every PID D satisfies the ACC, i.e. it is Noetherian.*

Proof. Let $I_1 \leq I_2 \leq \cdots$ be an ascending chain of ideals of D. Let $A = \bigcup_{i=1}^{\infty} I_i$.
We first claim that A is an ideal of D. Given $a, b \in A$, there are $i, j \in \mathbb{N}$ such that $a \in I_i$, and $b \in I_j$. WLOG we may assume $j \leq i$. Since the ideals satisfy $I_j \leq I_i$, we have $a, b \in I_i$, and I_i being an ideal, yields $a + b \in I_i$, so $a + b \in A$. For $r \in D$, we have $ra \in I_i$, so $ra \in A$.
Since D is a PID, there is $a \in A$ such that $A = \langle a \rangle$. But then there is $i \in \mathbb{N}$ such that $a \in I_i$, and therefore

$$\langle a \rangle \leq I_i \leq A = \langle a \rangle,$$

which yields $I_i = A$. For any $k \geq i$, we have

$$I_i \leq I_k \leq A = I_i,$$

so $I_k = I_i$. ∎

02/22/16

Proposition 5.1.6 *Let F be a field.*

1. *Every linear polynomial in $F[x]$ is irreducible.*
2. *For $f \in F[x]$, with $\deg(f) > 1$, if f has a root in F then it is reducible in $F[x]$.*
3. *For $f \in F[x]$, with $\deg(f) = 2$ or 3, f is reducible in $F[x]$ iff it has a root in F.*

Example 5.1.5. The polynomial $x^4+5x^2+6 \in \mathbb{Q}[x]$ is reducible, yet it has no root in $\mathbb{Q}$. It factors as $x^4+5x^2+6 = (x^2+2)(x^2+3)$.

Lemma 5.1.7 *1. Let $u, v \in D$. uv is a unit iff u and v are units.*

2. *Let $a_1, \ldots, a_n \in D$, and $p \in D$ be prime. If $P|a_1 \cdots a_n$ then $p|a_i$ for some $i = 1, \ldots, n$.*

3. *Let $p, q \in D$ such that p is irreducible and q is nznu. If $q|p$ then $p \sim q$.*

Proposition 5.1.8 *Let D be an integral domain satisfying*

1. *ACC, i.e D is Noetherian,*

2. *Every irreducible in prime.*

Then D is a UFD.

Proof. ■

From this proposition, together with Propositions **??** and 5.1.4.2, we get the following corollary.

Corollary 5.1.9 *Every PID is a UFD.*

This is the last implication needed to complete the proof of Theorem 5.0.1. The following example shows that this implication is strict.

Example 5.1.6. $\mathbb{Z}[x]$ is not a PID. It follows from Theorem 5.1.10 below, that it is a UFD. Let

$$I = \{f \in \mathbb{Z}[x] | \text{ constant term is even}\}.$$

It is easy to see that I is an ideal of $\mathbb{Z}[x]$, but there is no polynommial $f \in \mathbb{Z}[x]$ that generates I. A non-constant f would not have the constant 2 as a multiple in $\mathbb{Z}[x]$. A constant f would have to be even to be in I, and would not have x as a multiple in $\mathbb{Z}[x]$.

02/25/16

greatest common divisor

We have already seen that when D is an integral domain, the ring $D[x]$ of polynomials over D is also an integral domain. One may ask what properties of D survive when we move to the larger ring $D[x]$. We have seen (see Example 5.1.1.2) that when F is a field, $F[x]$ even though it is not a field, it is an Euclidean Domain. Example 5.1.6 above shows that the properties ED and PID do not survive in general. We will prove that the property of UFD does survive.

Theorem 5.1.10 *If D is a UFD, then the ring $D[x]$ of polynomials over D is a UFD.*

Corollary 5.1.11 *If D is a UFD then the ring $D[x_1, \ldots, x_n]$ of polynomialas in several variables over D is a UFD.*

We will need several lemmas and propositions before we can prove this theorem.

Definition 5.1.8. Let $a, b, d \in D$. We say that d is a *greatest common divisor* of a and b provided:

- d is a common divisor, i.e.

$$d|a \text{ and } d|b,$$

- if d' is a common divisor of a and b then $d'|d$, i.e.

$$d'|a \text{ and } d'|b \Rightarrow d'|d.$$

Lemma 5.1.12 *Greates common divisor of a and b is unique, up to associates, when it exists.*

We will denote by g.c.d.(a, b) "*the*" greatest common divisor of a and b when it exists, understanding that it is well defined up to associates.

Lemma 5.1.13 *Let D be an ID, $a, b, u \in D$.*

1. g.c.d.$(a, b) \sim$ g.c.d.(b, a), *whenever one of them exists,*

content
primitive

2. g.c.d.$(a, 0) \sim a$,
3. *if* u *is a unit* g.c.d.$(a, u) \sim 1$,
4. *if* $a|b$ *then* g.c.d.$(a, b) \sim a$.

In general, g.c.d.(a, b) does not have to exist. We will show that in a UFD it does always exist. Because of Lemma 5.1.13 we only need to consider the case when a and b are nznu.

Lemma 5.1.14 *Let D be a UFD, $a, p \in D$, nznu.*

1. *If p is irreducible, then it is prime.*
2. *There are finitely many (up to associates) irreducible divisors of a.*

Proof. ■

Proposition 5.1.15 *Let D be a UFD, $a, b \in D$ nznu.*
Let $p_1, \ldots, p_r$ be the list, without repetitions of all irreducible factors of either a or b, up to associates. Write

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad \alpha_i \geq 0 \tag{5.1}$$
$$b = p_1^{\beta_1} \cdots p_r^{\beta_r}, \qquad \beta_i \geq 0 \tag{5.2}$$
$$\tag{5.3}$$

Then a and b have a greatest commond divisor, and

$$\text{g.c.d.}(a, b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}, \quad \textit{where} \qquad gamma_i = \min\{\alpha_i, \beta_i\}$$

Proof. ■

Corollary 5.1.16 *Let $a, b, c \in D$.* g.c.d.$(ac, bc) \sim c \cdot$ g.c.d.(a, b).

Definition 5.1.9. Let D be a UFD, $0 \neq f \in D[x]$ with

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

The *content* of f, denoted $c(f)$ is defined as g.c.d.$(a_0, \ldots, a_n)$. Note that it is well-defined up to associates. We say that f is *primitive* if $c(f) \sim 1$.

Example 5.1.7. If we take $f = 3x^2 - 12x + 9 \in \mathbb{Z}[x]$ then $c(f) \sim 3$. Note that $f = 3(x^2 - 4x + 3)$ and the second factor is primitive. This holds in general.

Lemma 5.1.17 *Let D be a UFD, $0 \neq f \in D[x]$, $0 \neq a \in D$.*

1. *$c(af) \sim a \cdot c(f)$.*
2. *There is a primitive $\hat{f} \in D[x]$ such that $f = c(f) \cdot \hat{f}$. This primitive is unique, up to associates, and $\deg(\hat{f}) = \deg(f)$.*
3. *If $f = a\hat{a}$ with $\hat{f}$ primitive, then $c(f) \sim a$.*

02/26/16

Proposition 5.1.18 [Gauss' Lemma] *Let D be a UFD, $0 \neq f, g \in D[x]$. If f and g are primitive, then fg is primitive.*

Proof. ■

Corollary 5.1.19 *Let D be a UFD, $0 \neq f, g \in D[x]$.*

$$c(fg) \sim c(f) \cdot c(g).$$

Proof. Let $\hat{f}, \hat{g} \in D$ be primitive such that $f = c(f)\hat{f}$ and $f = c(g)\hat{g}$. Then $fg = c(f)c(g)\hat{f}\hat{g}$. By Gauss's lemma $\hat{f}\hat{g}$ is primitive, so by Lemma 5.1.17 we get $c(fg) \sim c(f) \cdot c(g)$, as desired. ■

The converse of Gauss' lemma follows from this corollary and Lemma 5.1.7.

Corollary 5.1.20 *Let D be a UFD, $0 \neq f, g \in D[x]$. fg is primitive iff f and g are primitive.*

Lemma 5.1.21 *Let D be a UFD, $f \in D[x]$ with $\deg(f) \geq 1$. If f is irreducible then it is prime*

Proof. Let $\hat{f} \in D[x]$ be primitive such that $f = c(f) \cdot \hat{f}$. Since f is irreducible, one of $c(f)$ and $\hat{f}$ is a unit. But $\deg(\hat{f}) = \deg(f) \geq 1$, so $\hat{f}$ is not a unit, so $c(f)$ is a unit, i.e. $c(f) \sim 1$. ■

Proposition 5.1.22 *Let D be a UFD, and Q its field of fractions. Let $p \in D$ and $f \in D[x]$ with $\deg(f) \geq 1$.*

1. *D is a subring of $D[x]$, and p is irreducible in D iff it is irreducible in $D[x]$.*
2. *$D[x]$ is a subring of $Q[x]$, and if f is irreducible in $D[x]$ then it is irreducible in $Q[x]$.*

Proof. ■

02/29/16

We now have all the ingredients needed to prove Theorem 5.1.10.

Theorem 5.1.10 *f D is a UFD, then the ring $D[x]$ of polynomials over D is a UFD.*

Proof. ■