KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-04-27

SANDRA DI ROCCO

CONTENTS

1. INTRODUCTION

In this section we will introduce the notion of further algebraic structures and prove the relation between them. We will define *Euclidean Domains* (ED) and prove that every Euclidean domain is a Principal ideal domain:

$$ED \Rightarrow PID.$$

We will also talk about *Unique factorization Domains* (UFD) and prove the relation

$$ED \Rightarrow PID \Rightarrow UFD$$

We will see that these are all strict arrows which cannot be inverted. In fact the search for examples of PID that are not Euclidean domains has led to interesting research in Algebra. Here is just an example. In the so called quadratic fields $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbb{Q}\}$, one defines the "integral elements" to be the elements $a + b\sqrt{d}$ such that the trace $a^2 - b^2d$ and the norm $2a$ are integers. The set of integral elements I_d is an ideal and

$$\mathbb{Z}[\sqrt{d}] \subseteq I_d \subset \mathbb{Q}(\sqrt{d}).$$

One would like to extend to I_d the theory of divisibility similar to the one for integers and thus wants to study when I_d is an ED, PID and UFD.

For $d < 0$ already in 1920 Dickson showed that I_d is a ED id and only if $d = -1, -2, -3, -7, -11$. For positive d the study continued in the 30s and 30 s and in 50 Davemport showed that I_d cannot be ED for $d > 2^{14}$. The problem was eventually solved: I_d is an ED (w.r.t the norm) if and only if $d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. In 1967 it was proven that I_d, $d < 0$ is a PID if and only if $d = -163, -67, -43, -19, -11, -7, -3, -2, -1$ so for example I_{-43} is a PID but not ED.

2. Euclidean Domains

Definition 2.1. An *Euclidean Domain* (ED) is an integral domain D endowed with an euclidean norm, that is a function $d : D \setminus \{0\} \to \mathbb{Z}$ such that

(1) $d(a) \leq d(ab)$ for all $a, b \neq 0$.
(2) For every $a \in D$ and $0 \neq b \in D$ there are $h, r \in D$ such that $a = bh + r$ with $r = 0$ or $d(r) < d(b)$.

We have already seen two (important) examples of Eucledeal domains, $\mathbb{Z}$ where $d(a) = |a|$, and $F[x]$ where $d(f(x)) = \deg(f(x))$.

Example 2.2. $\mathbb{Z}[i]$ is a ED with $d(z = n + im) = n^2 + m^2 = |z|$. (Section 47 in the book). If F is a field, then F is a ED with norm $d(a) = 0$, for all $a \in F$.

Proposition 2.3. (1) *Every Euclidian Domain is a PID.*
(2) *For every $a, b \in D$ there is a $c \in D$ such that $(a) + (b) = (c)$.*

Proof. Let $0 \neq I \subset D$ be a proper ideal of an Euclidian domain D and let $0 \neq b \in I$ be an element of minimal norm. Then every other element $a \in D$ an be written as $a = bh + r$ where r is necessarily 0 which implies that $I = (b)$. It follows that $(a) + (b) = (c)$, for some $c \in D$. □

Notice that $c/a, b$ and every other common divisor divides c. It is than a "biggest common divisor". Notice that it is NOT UNIQUE but is it uniquely defined up to a multiplication with a unit. In fact it is $(c) = (x)$ if $a = xu$ for an unit u.

Observe also that from what said above it follows that 1 is the elemend of minimal norm and that $u \in D$ is a unit if and only of $d(u) = 1$. In factif u is a unit then $d(u) \leq d(uu^{-1}) = d(1)$ and thus $d(u) = d(1)$.

3. Unique Factorization Domains

Recall that (Lecture 10) an element $a \in D$ for a PID D is prime if and only if it is irreducible. We will call two element a, b associates if $a = bu$ for a unit u.

Definition 3.1. A domain D is a *unique factorization domain* (UFD) if

- Every $0 \neq a \in D$ which is not a unit there is a unit $u \in D^*$ and a finite number of irreducible elements $q_1, \ldots, q_r \in D$, such that
$$a = uq_1 \cdots q_r.$$
- this factorization is unique up to ordering and associates.

Notice also that every irreducible element in a UFD is prime. In fact if $a|bc$, i.e. $bc = ak$ then by decomposing we have $b_1 \cdots b_k c_1 \cdots c_r = ad_1 \cdots d_l$ which implies that a is an associate of some b_i or some c_i and thas a/b or a/c. Because every prime is irreducible this means that in a UFD every element is a product of primes. Moreover observe that:

Lemma 3.2. *Let D be a domain, if every element is a product of primes then this decomposition is automatically unique up to a unit, i.e. it is a UFD*

Proof. Assume $a_1 \cdots a_k = b_1 \cdots b_s$. Proceed by induction on k. If $k = 1$, then $a_1 = ub_1$ because a_1 is irreducible. Assume $k > 2$, then a_1/b_i for some i, say $i = 1$. By cancellation property we have then $a_2 \cdots a_k = l_1 \cdot b_2 \cdot b_s$ and we are dome by induction. □

We know that $\mathbb{Z}$ is a UFD. Another important example is the $F[x]$ where F is a field. We will now show that every PID is a UFD. In what follows we will assume that D is a PID.

Lemma 3.3. *Let $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ be and infinite ascending chain of ideals of a PID D. Then the chain stabilizes, i.e. there exist N such that $I_m = I_N$ for $m > N$.*

Proof. It is straight forward to see that $I = \cup I_i$ is an ideal and thus it is $I = \cup I_i = (a)$, for some $a \in D$. But if $a \in I$ then $a \in I_N$ for some N and $a \in I_m$ for all $m > N$. This mean that $(a) \subset I_m$, for all $m \leq N$ and $I_k \subset (a) = I$ for all k. It follows that $(a) = I_N = I_m$ for all $m > N$. □

Rings for which Lemma 3.3 holds are called *Noetherian rings*. Note that it is not true that discending chains stabilize, for example in $\mathbb{Z}$,

$$... \subset (2^n) \subset \ldots \subset (8) \subset (4) \subset (2) \subset (1).$$

Theorem 3.4. *Every PID is a UFD.*

Proof. Let D be a PID and let S the non-zero elements which are not units and which cannot be factored in a finite product of prime elements. Assume that S is not empty and let $a \in S$. Let (c) be a maximal ideal containing (a). Then c is irreducible and c/a. This means that for every element $a \in S$ we can choose a divisor $c_a|a$ and a uniquely determined x_a such that $a = c_a x_a$.

Observe that x_a cannot be a unit because otherwise a would be irreducible and must belong to S otherwise would have a factorization and thus a would have one. It follows that $x_a \in S$ and $(a) \subset (x_a)$ is a proper inclusion, in fact if $(a) = (x_a)$ then $x_a = ay$ for some $y \in D$ and thus $a = x_a c_a = ayc_a$ which implies $yc_a = 1$ which is impossible since c_a is irreducible.

The above reasoning shows that we can define a function $f : S \to S$ as $f(a) = x_a$. Moreover by recursion we can define a function $\phi : \mathbb{Z} \to S$ as

$$\phi(0) = a, a_{n+1} = \phi(n+1) = f(\phi(n)) = x_{\phi(n)}.$$

This produces an ascending chain of ideals

$$(a) \subset (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$$

which does not stabilizes. But this contradicts Lemma 3.3. it follows that S is empty and thus every non-zero element has a factorization.

Assume that $a = c_1 \cdots c_n = d_1 \cdots d_m$ where the c_i, d_j are irreducible and thus prime. Then every c_i divides some d_j. By changing the order we can assume that $i = j = 1$ and $c_1 = d_1 u_1$. Notice that if c_1/u_1 then c_1 would be invertible contraddicting the fact that it is prime. Then c_1/d_1 and thus u_1 must be a unit. Then

$$d_1 u_1 \cdots c_n = d_1 \cdots d_m$$

By the cancellation low we have that $u_1c_2\cdots c_n = d_2\cdots d_m$. By induction on the length of the decomposition we conclude that $n-1=m-1$. □

4. POLYNOMIAL RING

Let us look at the following problem: When is a finetely generated ideal contained in a principal ideal?

Lemma 4.1. *Let D be a UFD and let $I=(a_1,\dots,a_k)$ be a finitely generated ideal. Then there is a minimal principal ideal $(d(I))$ containing I.*

Proof. Let d be the product of the common primes in the decomposition of the a_i's. Assume that $I\subset(d')$, then d'/a_i for $i=1,\dots,k$ and thus by definition d'/d, i.e. $(d)\subset(d')$. □

Definition 4.2. A finitely generated ideal $I=(a_1,\dots,a_k)\subset D$ is called primitive if $(d(I))=D$. A polynomial $f=\sum a_i^k x^i\in D[x]$ is called primitive if $I=(a_1,\dots,a_k)$ is primitive.

Moreover the content of a polynomial $f=\sum a_i^k x^i\in D[x]$ is $c(f)\in D$ where $c(d)=d(I)$, for $I=(a_1,\dots,a_k)$

Notice that every polynomial $f(x)$ can be then written as $f(x)=c(f)g(x)$ where $g(x)$ is primitive. Recall that:

Lemma 4.3. *Let R be a ring and let $P\subset R$ be a prime ideal. Let I,J be ideals such that $IJ\subset P$ Then $I\subset P$ or $J\subset P$.*

Proof. Assume I not contained in P, then there is an element $a\in I$ and $a\notin P$. But $aJ\subset P$ and because P is prime this implies $J\subset P$. □

Corollary 4.4. *(GAUSS LEMMA) Let D be a UFD. The product of two primitive elements is primitive.*

Proof. Assume $I=(a_1,\dots,a_k)$, $J=(b_1,\dots,b_s)$ primitive. We have to prove that IJ is primitive. If not there is a proper principle ideal containing it , $IJ\subset(d)$. Let $d=\Pi p_i$, then $IJ\subset(d)\subset(p_i)$ and by Lemma 4.3 $I\subset(p_i)$ or $J\subset(p_i)$ which is impossible because they are primitive. □

Theorem 4.5. *If D is a UFD then $D[x]$ is a UFD.*

Proof. Because $D[x]$ is a domain we just have to show that every element is a product of primes and then the statement will follow by Lemma 4.3. Let K be the field of fractions of D. Let $f(x)\in D[x]\subset K[x]$. Recall that $K[x]$ is a PID and therefore by Theorem 3.4 a UFD. Then we can decompose

$$f(x)=F_1(x)\cdots F_k(x) \text{ where } F_i(x) \text{ are primes in } K[x].$$

After "clearing the denominator" we can write:

$$df(x)=g_1(x)\cdots g_k(x)=c(g_1)\cdots c(g_k)\Pi f_i(x) \text{ in } D[x],$$

where the f_i are primitive polynomials.

We will show that f_i are prime in $D[x]$ from which the statement will follow.

Consider the map of rings:

$$\phi : D[x]/(f_i) \to K[x]/[(F_i) = (f_i)].$$

It is an injective map. In fact let $h(x) \in D[x]$ so that $h(x) \in (F_i)$ in $K[x]$. Then $h(x) = F_i(x)G(x)$ after clearing the denominators we have

$$Ah(x) = g_i(x)H(x) = c(f_i)c(H)f_i(x)g(x).$$

Let $A = \Pi p_j$, then p_j cannot divide $f_i(x)g(x)$ since it is primitive by Lemma 4.3. Then $p_j/c(f_i)c(H)$ and thus by cancellation we obtain:

$$h(x) = Bf_i(x)g(x)$$

which implies that $h(x) \in (f_i)$. The map ϕ being injective implies that $D[x]/(f_i)$ is a subring of a domain:$K[x]/[(F_i)$ and thus a domain. It follows that (f_i) is prime for all i.

Now consider again $df(x) = c(g_1)\cdots c(g_k)\Pi f_i(x)$. Every prime p_i dividing d cannot divide $\Pi f_i(x)$ since they are primitive and therefore have to divide $c(g_1)\cdots c(g_k)$. By cancellation we obtain $f(x) = C\Pi f_i(x)$. Let $C = \Pi q_j$ be the prime decomposition, it follows then that

$$f(x) = \Pi q_j \Pi f_i(x),$$

a prime decomposition. □

By induction one sees that $D[x_1, \dots, x_k]$ is a UFD. We have showed that $\mathbb{Z}[x]$ is not a PID but it is a UFD. So the arrow in Theorem 3.4 cannot be reversed.

RECOMMENDED EXCERCISES

- IX-45 1-8,25,26,29,30,31.
- IX-46 1-5, 15, 16, 17. 19.
- IX-47 1-5,10,11,14,15.