LECTURE 10 : PRINCIPAL IDEAL DOMAINS

Let's review, last time we introduced norms on rings and Euclidean domains. We also defined associates, irreducible and prime elements. This material is my old Lectures 27 & 28 which largely corresponds to § 8.1 and 8.2 of DSF. Today we should work more with primes & irreducible elements and how the norm for $\mathbb{Z}[\sqrt{D}]$ etc. produces nice examples.

Th^{m} (4.7.8) In an integral domain every prime is an irreducible

Th^{m} 4.7.9 Let R be a commutative ring with 1. If a, b are associates then $(a) = (b)$. Furthermore, if R is an integral domain and $I = (a)$ and $I = (b)$ then a & b are associates.

We proved these last class. Sometimes Th^{m} 4.7.9 still works outside the context that I is an integral domain.

E1 $R = \mathbb{Z}_6$ then $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$ and $2(5) = 10 = 4$

$2 \not\sim 4$ are associates.

Th^{m} In a Principal Ideal Domain (PID) an element is prime $\iff$ an element is irreducible

PROOF: Let D be a PID, then D is an integral domain in which every ideal is generated by a single element.

$\Rightarrow$ Suppose $a \in D$ is prime $\Rightarrow$ a is irreducible by Th^{m} 4.7.8. //

$\Leftarrow$ Suppose a is irreducible. Then suppose $a \mid bc$ for some $b, c \in D$. Let

$$I = \{ ax + by \mid x, y \in D \}$$

then I is an ideal hence $\exists\, d \in D$ for which $(d) = I$.
Observe $a = a(1) + b(0) \in I$ thus $a = rd$ for some $r \in D$.
But, a is irreducible $\therefore$ r or d is a unit.

⇐ Continued, we supposed a irreducible and $a \mid bc$ and we found $a = rd$ where r or d was unit.

(i.) If d is a unit then $1 = dd'$ hence $1 \in I = \{ax+by \mid x,y \in D\}$ and thus $c = c(ax+by) = acx + (bc)y$ which implies $a \mid c$ since $a \mid acx$ and $a \mid bc$ was given.

(ii.) If r is a unit then $a = rd \Rightarrow a$ & r are associates hence $\langle d \rangle = \langle a \rangle = I \Rightarrow b = a(0) + b(1) \in I$ thus $b = a\lambda$ for some $\lambda \in D \therefore a \mid b$.

Consequently $a \mid bc \Rightarrow a \mid c$ or $a \mid b \therefore a$ is prime. //

E2 $\mathbb{Z}$ is a PID where $I = (n)$ for some $n \in \mathbb{Z}$. On the other hand $\mathbb{Z}[x]$ is not a PID since $I = (2, x)$ can be shown to not be principal, that is, $\nexists\, d(x) \in \mathbb{Z}[x]$ for which

$$(d(x)) = \{ d(x)f(x) \mid f(x) \in \mathbb{Z}[x] \}$$
$$= \{ 2g(x) + xh(x) \mid g(x), h(x) \in \mathbb{Z}[x] \}$$

WHY?

Suppose $x \in (d(x))$ and $2 \in (d(x))$ then $x = d(x)g(x)$ * and $2 = d(x)h(x)$ ** for some $g(x), h(x) \in \mathbb{Z}[x]$. Notice $g(x), h(x) \neq 0$ since $2, x \in (2, x)$ by construction.

evaluate * at $x = 0$; $0 = d(0)g(0)$

evaluate ** at $x = 0$; $2 = d(0)h(0)$

Thus $d(0), h(0) \neq 0 \Rightarrow g(0) = 0 \Rightarrow g(x) = c_1 x + \cdots$

Hence $x = d(x)(c_1 x + \cdots) \Rightarrow d(0) = \pm 1,\ c_1 = \pm 1 \Rightarrow (d(x)) = \mathbb{Z}[x]$.

But, clearly $(2, x) \neq \mathbb{Z}[x]$ since $1 + x \notin (2, x)$.

PROPOSITION 1: EVERY IDEAL IN A EUCLIDEAN DOMAIN IS PRINCIPAL. IN FACT, IF $I \neq 0$ IS AN IDEAL IN A EUCLIDEAN DOMAIN THEN $I = (d)$ WHERE d is any nonzero element of I of minimum norm.

PROOF: let D be a Euclidean Domain with norm N. If $I \neq 0$ is an ideal in D then $S = \{N(x) \mid x \in I\}$ is a nonempty subset of $\mathbb{N} \cup \{0\}$. Thus by Well-Ordering-Principle S has smallest member s_0, hence $\exists\, x_0 \in I$ with $N(x_0) = s_0$. Let $z \in I$ and apply the division algorithm in D to select $q, r \in D$ with $0 \leq N(r) < N(x_0)$,

$$z = qx_0 + r$$

Note $z \in I$ and $qx_0 \in I$ since $x_0 \in I$ thus

$$r = z - qx_0 \in I$$

Hence $r = 0$ as $r \neq 0$ would $\not\rightarrow$ minimality of $N(x_0)$. Thus $z \in I \Rightarrow z = qx_0 \in (x_0) \therefore I \subseteq (x_0)$ and conversely, $(x_0) \subseteq I$ is clear since $x_0 \in I$ an ideal. Thus $(x_0) = I$. Finally, $(0) = \{0\}$. //

Corollary: R a Euclidean Domain $\Rightarrow R$ IS A PID

E3 $\mathbb{Z}[x]$ is not a Euclidean Domain for <u>any</u> choice of norm since $(2, x) \neq (d(x))$ for any $d(x) \in \mathbb{Z}[x]$. That is, $\mathbb{Z}[x]$ IS <u>NOT</u> A PID.

GCD IN EUCLIDEAN DOMAINS

Let's review the definition of divisible, multiple etc.

Def^n/ Let R be commutative ring with $a, b \in R$, $b \neq 0$

(1.) a is <u>multiple</u> of b if $a = br$ for some $r \in R$ then we say b divides a and write $b \mid a$.

(2.) A <u>greatest common divisor</u> (gcd) of a and b is a nonzero $d \in R$ such that

(i.) $d \mid a$ and $d \mid b$

(ii) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

<u>Notation</u>: $\gcd(a,b) = d = (a,b)$

anticipates $(d) = (a,b)$ for ideals.

Likewise, at level of ideals,

$$b \mid a \iff a \in (b) \iff (a) \subseteq (b)$$

$$d \mid a \text{ and } d \mid b \implies (d) \text{ contains both } a \text{ and } b$$
$$\therefore (a,b) \subseteq (d)$$

$$d' \mid d \iff (d) \subseteq (d')$$

Hence,

<u>PROPOSITION 2</u>: If $a, b \neq 0$ in a commutative ring R such that $I = (a,b) = (d)$ then d is a g.c.d. of a and b.

<u>Remark</u>: we should generally say $d \in \gcd(a,b)$ and think of $\gcd(a,b)$ as the <u>set</u> of g.c.d.'s of a and b. For $\mathbb{Z}$, $\mathbb{Z}^\times = \{-1, 1\}$ so the ambiguity is small, but more units in $R \Rightarrow$ greater ambiguity.

Th^{m}(4) p. 275 D&F §8.1 / **(Prop 6 of §8.2 D&F)**

Let R be a Euclidean Domain and a, b nonzero elements in R. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm for a, b. Then

(1.) d is a g.c.d. of a & b

(2.) the principal ideal $(d) = (a, b)$ thus $\exists\, x, y \in R$ for which $d = ax + by$

(3.) d is unique up to mult. by unit.

Proof: see p. 275 of D&F, it echoes proof for Euclidean Algo. given for $\mathbb{Z}$ in other courses. //

PROP. 7 / Every nonzero prime ideal in a PID is a maximal ideal

PROOF: p. 280 of D&F. Perhaps we'll do in-class. //

Corollary 8 / If R is any commutative ring s.t. the polynomial ring $R[x]$ is a PID (or Euclidean Domain) then R is necessarily a field.

Proof: If $R[x]$ is a PID then since R is subring of $R[x]$ we see R must be an integral domain in order for $R[x]$ to be integral domain. Then note (x) is a nonzero prime ideal in $R[x]$

Since $R[x]/(x) \cong R$ ← (given to be integral domain hence (x) is prime ideal)

Then by Prop 7, (x) is maximal ideal and thus R must be a field. //

EXAMPLES ILLUSTRATING PID VS. UFD VS. EUCLIDEAN DM.

We don't know what a UFD is just yet, but some of the examples below will alert us to the issue...

E4 $(2, x)$ is nonprincipal ideal within $\mathbb{Z}[x]$

E5 $(2, x)$ is a principal ideal within $F[x]$ where F a fidd since $F[x]$ is Euclidean Domain $\Rightarrow$ $F[x]$ is PID.

E6 (Ex 4.7.2 of my LECTURE 27)

$1+\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ with $N(a+b\sqrt{-3}) = a^2+3b^2$

Suppose $1+\sqrt{-3} = xy$ then since $N(zw) = N(z)N(w)$

$$N(1+\sqrt{-3}) = N(x)N(y)$$

Lemma: $N(\text{unit}) = 1$

$$4 = N(x)N(y)$$

$\Rightarrow N(x) = 2$ and $N(y) = 2$ if both x and y are not units

But $N(a+b\sqrt{-3}) = a^2+3b^2 = 2$ has no integer solutions $\therefore$ x or y must be unit

Hence $1+\sqrt{-3}$ is irreducible in $\mathbb{Z}[\sqrt{-3}]$

Observe that

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 1-(-3) = 4 = (2)(2)$$

Thus $1+\sqrt{-3} \mid (2)(2)$ yet $1+\sqrt{-3} \nmid 2$ since,

$$(1+\sqrt{-3})(a+b\sqrt{-3}) = 2 \Rightarrow a-3b+(b+a)\sqrt{-3} = 2$$

$$\Rightarrow a-3b = 2 \text{ and } b+a = 0$$

$$\Rightarrow a = -b \text{ and } 4a = 2$$

$$\Rightarrow a = 1/2 \in \mathbb{Z} \quad \rightarrow\leftarrow$$

Therefore, $1+\sqrt{-3}$ IS NOT PRIME.

$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ IS NOT A PID.

E7 $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ is a PID which is <u>not</u> a Euclidean Domain.

E8 Can show $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$ since

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

is divisible by 3 yet $3 \nmid (2 \pm \sqrt{-5})$.

Again $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

<u>Ultimately we want to understand:</u>

fields $\subset$ Euclidean Domains $\subset$ PIDs $\subset$ UFDs $\subset$ integral domains

$\mathbb{Z}[x]$ $\mathbb{Z}[\sqrt{-5}]$

(all containments above are proper)

4.8 Lecture 28: divisibility in integral domains II

In this Lecture we complete our study of Chapter 18 of Gallian. Here we explore the interplay between Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains.

Definition 4.8.1. *Let D be an integral domain. Then D is said to be a* **Euclidean Domain** *if there is a norm N on D such that for any two elements $a, b \in D$ with $b \neq 0$ there exists elements $q, r \in D$ with*

$$a = qb + r$$

and $r = 0$ or $N(r) < N(b)$. We call q the **quotient** *and r the* **remainder** *of the division.*

You can contrast the definition above to that which is given in Gallian. In part, a Euclidean Domain is an integral domain D with a function $d : D \to \mathbb{N} \cup \{0\}$ such that $d(a) \leq d(ab)$ for all $a, b \neq 0$ in D. If we have a positive norm for which $N(xy) = N(x)N(y)$ then define $d(x) = N(x)$ and note:

$$d(ab) = N(ab) = N(a)N(b) = d(a)d(b)$$

and as $a, b \neq 0$ we have $d(a), d(b) \in \mathbb{N}$ thus $d(a) = d(ab)/d(b) \leq d(ab)$. In short, if we have a positive multiplicative norm then it provides a measure (in the langauge of Gallian page 321). I should caution, we do not assume all norms are multiplicative, see Example 4.8.3.

We should notice a Euclidean Domain does not generally come with a division algorithm which produces a unique quotient and remainder. Even the integers allow for non-unique quotient and remainder in a division. Notice Theorem 4.7.5 applies to norms for rings other than $\mathbb{Z}[\sqrt{d}]$ for d square-free. If N is a norm which is positive and multiplicative then we satisfy (i.) and (ii.) of Theorem 4.7.5 hence (iii.) and (iv.) follow since the proof of (iii.) and (iv.) simply require the verity of (i.) and (ii.).

Example 4.8.2. *Consider $D = \mathbb{Z}$ with $N(x) = |x|$. It is simple to see N defines a positive norm and $N(xy) = |xy| = |x||y| = N(x)N(y)$ for all $x, y \in \mathbb{Z}$. Notice $|u| = 1$ implies $u = \pm 1$. The units in $\mathbb{Z}$ are just $1, -1$. Let me give an explicit example to make the ambiguity of the division algorithm a bit more explicit. Consider $a = 54$ and $b = 8$ we have:*

$$54 = 6(8) + 6 \qquad or \qquad 54 = 7(8) - 2.$$

Now, in the context of the integers the use of a positive remainder is what is usually done.

I merely mean to indicate that even in $\mathbb{Z}$ the division algorithm may not be unique.

Example 4.8.3. *If F is a field then $D = F[x]$ is a Euclidean Domain where we define $N(f(x)) = deg(f(x))$. Since $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$ we don't have a multiplicative norm. The units of D are nonzero constant polynomials which have $N(f(x)) = N(c) = 0$.*

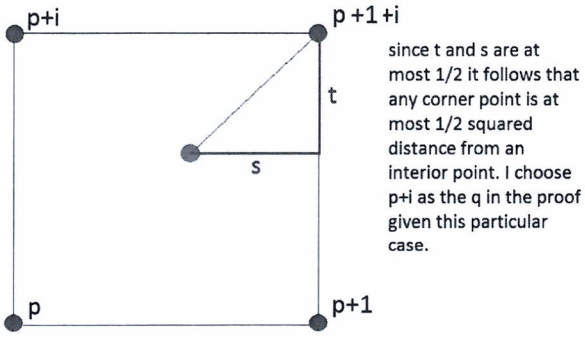
Example 4.8.4. *The Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ form a Euclidean Domain with $N(a + ib) = a^2 + b^2$. It is easy to prove $N(zw) = N(z)N(w)$ and $N(z) = 0$ iff $z = 0$ hence $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ forms a multiplicative norm. The proof that $\mathbb{Z}[i]$ is a Euclidean Domain with respect to N is a bit involved. I'll let you read page 322-323 for Gallian's proof. I'll sketch a similar proof here. To divide $a+ib$ by $c+id$ we may accomplish this explicitly in $\mathbb{C}$ as $z = \frac{a+ib}{c+id}$ is a complex number. The Gaussian integers from a lattice of points and we simply pick one of the four points in $\mathbb{Z}[i]$ which are closest to z and call it q. Define $r = a+ib-q(c+id)$ then clearly $a+ib = q(c+id)+r$ and as*

$$\frac{a+ib}{c+id} = z = q + \frac{r}{c+id}$$

by the construction of q, worst case scenario we find z as the center point of a cell in the $\mathbb{Z}[i]$ lattice. Notice the center point is distance $1/\sqrt{2}$ from each of the closest 4 points. Thus:

$$\left|\frac{r}{c+id}\right| < \frac{1}{\sqrt{2}} \quad \Rightarrow \quad |r| < \frac{|c+id|}{\sqrt{2}} \quad \Rightarrow \quad N(r) < N(c+id)/2.$$

Perhaps the following picture helps explain the proof in the Example above:



No matter where $\frac{a+ib}{c+id}$ lands in the complex plane the closest point in $\mathbb{Z}[i]$ will be within $1/\sqrt{2}$ distance. When we study other $\mathbb{Z}[\sqrt{-d}]$ for $d > 0$ the geometry of this argument is spoiled. There is much to learn about Euclidean Domains which is not emphasized in Gallian. Familar algorithms and concepts in $\mathbb{Z}$ have natural generalizations to abstract Euclidean Domains. For example, we can execute the Euclidean Algorithm in $\mathbb{Z}[i]$ just as we do in $\mathbb{Z}$ by systematically removing first the divisor, then the remainder, then the remainder of the remainder's division etc...

Example 4.8.5. *Consider $\alpha = 11 + 3i = a + ib$ and $\beta = 3i + 2 = c + id$ (a, b, c, d notation in reference to the proof above). Let's walk through the Euclidean Algorithm in vector format: in each step I have to do side calculation (not shown) to decide which multiple of the previous remainder should be subtracted to make the difference minimal. If I don't see it by inspection then I follow the method of the proof.*

$$(11 + 3i, 3i + 2) = (\alpha, \beta)$$
$$(3i + 2, 1 + i) = (\beta, \alpha - (2 - 2i)\beta)$$
$$(1 + i, -i) = (\alpha - (2 - 2i)\beta, \beta - (3 + i)[\alpha - (2 - 2i)\beta])$$

at which point we stop since $-i$ is a unit in $\mathbb{Z}[i]$. Thus,

$$-i = \beta - (3 + i)\alpha + (3 + i)(2 - 2i)\beta$$

or

$$-i = (9 - 4i)\beta - (3 + i)\alpha$$

hence

$$1 = (4 + 9i)(3i + 2) + (1 - 3i)(11 + 3i).$$

This calculation shows the greatest common divisor of $11 + 3i$ and $3i + 2$ is 1, or, you could say $-1, i, -i$. In fact, to study this properly we need to embrace the concept that the gcd is an ideal. In this case,

$$\langle 11 + 3i \rangle + \langle 3i + 2 \rangle = \langle 1 \rangle = \mathbb{Z}[i]$$

The ideals $\langle 11+3i \rangle$ and $\langle 3i+2 \rangle$ are **comaximal** *since there sum is the entire ring. Comaximal ideals are the ideal version of relatively prime. Note, two integers a, b are relatively prime if $gcd(a, b) = 1$ which implies $ak + bl = 1$ hence $x = akx + blx$ for each $x \in \mathbb{Z}$ and thus $\langle a \rangle + \langle b \rangle = \mathbb{Z}$.*