Lecture 18: Euclidean domains

Thursday, November 29, 2018 9:20 AM

The main reason that we have a very good understanding of ideals of $\mathbb{Z}$ is because of the division algorithm. That is our main motivation for the following definition.

Def. An integral domain D is called a **Euclidean Domain** if

$\exists N: D \to \mathbb{Z}^{\geq 0}$, (1) $N(d) \geq 0$, $N(d)=0 \iff d=0$.

(2) $\forall a,b \in D \setminus \{0\}$, $\exists q, r \in D$ s.t.

$a = bq + r$ and $N(r) < N(b)$.

(q is called a quotient of a divided by b, and r is called a remainder of a divided by b.)

Ex. Division algorithm implies $\mathbb{Z}$ is a ED. Here $N: \mathbb{Z} \to \mathbb{Z}^{\geq 0}$,

$N(a) := |a|$ works.

Ex. Suppose F is a field. Then one can run the long division algorithm in $F[x]$, and deduce $\forall a, b \in F[x] \setminus 0$, $\exists q, r \in F[x]$ s.t.

$a = bq + r$ and $\deg r < \deg b$. And so $N: F[x] \to \mathbb{Z}^{\geq 0}$,

$N(a) := 2^{\deg a}$ with the convention that $2^{-\infty} = 0$ shows us that $F[x]$ is a E.D.

Lecture 18: Gaussian integers form a ED

Thursday, November 29, 2018 11:17 AM

Proposition $\mathbb{Z}[i] := \{a+bi \mid a,b\in\mathbb{Z}\}$ is a E.D..

Pf. (Check that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.)

Let $a,b\in\mathbb{Z}[i]\setminus 0$. Let $z := \frac{a}{b}\in\mathbb{C}$. Notice that $\mathbb{Z}[i]$ is a lattice in $\mathbb{C}$, and $\mathcal{F} := \{z'\in\mathbb{C} \mid |\mathrm{Re}(z')|, |\mathrm{Im}(z')| \le 1/2\}$ is a fundamental region of $\mathbb{Z}[i]$; that means

$$\mathbb{C} = \mathbb{Z}[i]+\mathcal{F} \quad \text{and} \quad |z''+\mathcal{F}\cap\mathcal{F}| = 0 \ \text{ if } z''\in\mathbb{Z}[i]\setminus 0.$$

(**Remark**. If X is a metric space, $\Gamma\subseteq \mathrm{Isom}(X)$ is a discrete subgroup, then for any $o\in X$ one can define

$$\mathcal{F}_o := \{x\in X \mid d(x,o) \le d(x,\gamma\cdot o) \ \forall \gamma\in\Gamma\};$$

then $X = \Gamma\cdot\mathcal{F}_o$; and $\mathcal{F}_o$ is called the Dirichlet fundamental region.)

Of course here we do not need this fancy language:

$z = \mathrm{Re}(z) + i\,\mathrm{Im}(z)$. $\mathrm{Re}(z) = q_1 + \varepsilon_1$ where $q_1\in\mathbb{Z}$, $|\varepsilon_1|\le 1/2$ and $\mathrm{Im}(z) = q_2+\varepsilon_2$ where $q_2\in\mathbb{Z}$, $|\varepsilon_2|\le 1/2$. So

$$\frac{a}{b} = \underbrace{(q_1+iq_2)}_{q\in\mathbb{Z}[i]} + (\varepsilon_1+i\varepsilon_2).$$ Hence $a = bq + \underbrace{b(\varepsilon_1+i\varepsilon_2)}_{r}$.

Lecture 18: ED implies PID

Thursday, November 29, 2018 11:31 AM

$\Rightarrow r = a - bq \in \mathbb{Z}[i]$ as $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

and $|r| = |b|\,|\varepsilon_1 + i\varepsilon_2| \leq |b|\sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{|b|}{\sqrt{2}}$.

Let $N: \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}$, $N(a) := |a|^2$. So by the above argument, $\forall a, b \in \mathbb{Z}[i] \setminus 0$, $\exists q, r \in \mathbb{Z}[i]$,

$a = bq + r$, $N(r) \leq N(b)/2 < N(b)$; which implies $\mathbb{Z}[i]$ is a E.D. ■

In a E.D. we get a very good understanding of ideals.

Def. An integral domain D is called a Principal Ideal Domain (PID) if any ideal is principal (that means any ideal is generated by one element.).

Theorem. E.D. $\Rightarrow$ PID.

Pf. Suppose $\mathcal{I} \triangleleft D$. If $\mathcal{I} = 0$, then it is principal. Suppose $\mathcal{I}$ is a non-zero ideal. Let $a_0 \in \mathcal{I}$ be such that

$N(a_0) = \min \{ N(a) \mid a \in \mathcal{I} \setminus \{0\} \}$. (Existence follows from the well-ordering principle of $\mathbb{Z}^{>0}$.)

Lecture 18: Irreducible, Prime, associates

Thursday, November 29, 2018 11:51 AM

Claim. $\mathcal{A} = \langle a_0 \rangle$.

Pf of Claim. $a_0 \in \mathcal{A} \Rightarrow \langle a_0 \rangle \subseteq \mathcal{A}$.

$\cdot\, a \in \mathcal{A} \Rightarrow \exists q, r \in D$, $a = a_0 q + r$ and $N(r) < N(a_0)$.

$r = a - a_0 q \in \mathcal{A}$
$N(r) < N(a_0)$
$N(a_0) = \min\{N(\acute{a}) \mid \acute{a} \in \mathcal{A} \setminus \{0\}\}$

$\Rightarrow r = 0 \Rightarrow a = a_0 q \in \langle a_0 \rangle$;

and so $\mathcal{A} = \langle a_0 \rangle$. ∎

We would like to do "number theory" and "arithmetic" with rings as we did with $\mathbb{Z}$. We would like to see in what extent we get prime factorizations.

Def. Let D be an integral domain.

(1) $a \in D$ is called <u>irreducible</u> if $a \neq 0$, $a \notin D^\times$, and

$$a = xy \Rightarrow x \in D^\times \text{ or } y \in D^\times.$$

(2) $a \in D$ is called <u>prime</u> if $a \neq 0$, $a \notin D^\times$, and

$$a \mid xy \Rightarrow a \mid x \text{ or } a \mid y.$$

(3) $a, b \in D$ are called <u>associates</u> if $\exists u \in D^\times$, $a = bu$; and we write $a \sim b$.

Lecture 18: These properties in terms of ideals

Thursday, November 29, 2018 12:09 PM

Lemma. Let D be an integral domain.

(1) $a \in D$ is irreducible $\iff$ $a \neq 0$ and $\langle a \rangle$ is maximal among proper principal ideals.

(2) $a \in D$ is prime $\iff$ $a \neq 0$ and $\langle a \rangle$ is prime.

(3) $a \sim b \iff \langle a \rangle = \langle b \rangle$; in particular $\sim$ is an equival. relation.

Pf. (1) ($\Rightarrow$) a irred. $\Rightarrow a \neq 0$ and $a \notin D^\times \Rightarrow a \neq 0$ and $\langle a \rangle \neq D$.

$\langle a \rangle \subseteq \langle b \rangle \subsetneq D \Rightarrow a \in \langle b \rangle \Rightarrow a = bc$

$\Rightarrow b \in D^\times$ or $c \in D^\times$ $\Rightarrow c \in D^\times$ $\Rightarrow b = c^{-1}a \in \langle a \rangle$

$\langle b \rangle \neq D \Rightarrow b \notin D^\times$

And so $\langle b \rangle \subseteq \langle a \rangle$. Therefore $\langle a \rangle = \langle b \rangle$.

($\Leftarrow$) $\langle a \rangle$ is proper $\Rightarrow a \notin D^\times$

$a = bc \Rightarrow \langle a \rangle \subseteq \langle b \rangle \Rightarrow \langle a \rangle = \langle b \rangle$ or $\langle b \rangle = D$. (by the max. cond.)

Case 1. $\langle a \rangle = \langle b \rangle \Rightarrow b = ac'$, and $b \neq 0$ as $a \neq 0$.

$\Rightarrow b = ac' = bcc'$

(cancellation) $\Rightarrow 1 = cc' \Rightarrow c \in D^\times$

Case 2. $\langle b \rangle = D \Rightarrow b \in D^\times$.

(And $a \neq 0$.)

Lecture 18: These properties in terms of ideals

Thursday, November 29, 2018 12:21 PM

(2) ($\Rightarrow$). $a \notin D^\times \Rightarrow \langle a \rangle \neq D$

. $bc \in \langle a \rangle \Rightarrow a \mid bc \Rightarrow a \mid b$ or $a \mid c$

$\Rightarrow b \in \langle a \rangle$ or $c \in \langle a \rangle$.

. $a \neq 0$

($\Leftarrow$) $\langle a \rangle \neq D \Rightarrow a \notin D^\times$.

. $a \neq 0$.

. $a \mid bc \Rightarrow bc \in \langle a \rangle \Rightarrow b \in \langle a \rangle$ or $c \in \langle a \rangle$

$\Rightarrow a \mid b$ or $a \mid c$.

(3) ($\Rightarrow$) $a \sim b \Rightarrow a = bu$ for some $u \in D^\times \Rightarrow \begin{cases} a \in \langle b \rangle \\ b = au^{-1} \in \langle a \rangle \end{cases}$

$\Rightarrow \begin{cases} \langle a \rangle \subseteq \langle b \rangle \\ \langle b \rangle \subseteq \langle a \rangle \end{cases} \Rightarrow \langle a \rangle = \langle b \rangle$.

($\Leftarrow$) If $\langle a \rangle = \langle b \rangle$, then $a = 0 \Leftrightarrow b = 0$.

. So w.l.o.g. we can and will assume $a \neq 0$ and $b \neq 0$.

$\langle a \rangle = \langle b \rangle \Rightarrow \begin{cases} a = bc \\ b = ac' \end{cases}$ for some $c, c' \in D \Rightarrow$

$b = ac' = bcc' \Rightarrow cc' = 1 \Rightarrow c \in D^\times \Rightarrow a \sim b$.

($b \neq 0$; $a = bc$)

One can easily check properties of an equivalence relation using (3). ∎

Lemma. Let D be an integral domain. Then $a \in D$ is prime implies that $a \in D$ is irreducible.

Lecture 18: Prime implies irreducible

Thursday, November 29, 2018 12:34 PM

Pf.. a is prime $\Rightarrow a \neq 0$ and $a \notin D^\times$.

$a = bc \Rightarrow a \mid bc \Rightarrow a \mid b$ or $a \mid c$. By symmetry we can and will assume $a \mid b$. Hence $b = ac'$; therefore

$$\left.\begin{array}{l} b = ac' = bcc' \\ a \neq 0 \Rightarrow b \neq 0 \end{array}\right\} \Rightarrow 1 = cc' \Rightarrow c \in D^\times.$$

■

In general converse of the previous lemma is NOT correct. Often it is easier to check if an element is irreducible; but it is not easy to show something is prime. In $\mathbb{Z}$, Euclid's lemma implies irreducible $\iff$ prime. Next we generalize this to any PID.

Proposition. Suppose D is a PID. Then

$$a \in D \text{ is irreducible} \iff a \in D \text{ is prime.}$$

Pf. ($\Leftarrow$) is a consequence of the previous lemma.

($\Rightarrow$) $a \in D$ irred. $\Rightarrow a \neq 0$ and $\langle a \rangle$ is maximal among proper principal ideal. Since all the ideals are principal, we deduce

that $\langle a \rangle$ is a maximal ideal; and so $\langle a \rangle$ is a prime ideal. As a is also $\neq 0$, we deduce that a is prime. ∎

To get that "prime $\Leftrightarrow$ irreducible" one does not need to assume D is a PID; for instance this property holds in $\mathbb{Z}[x]$; but $\mathbb{Z}[x]$ is not a PID (we will see both of these claims later.)

The key point is the Uniqueness of Factorization into irred.

Def. An integral domain D is called a Unique Factorization Domain (UFD) if $\forall\, a \in D \setminus (\{0\} \cup D^\times)$,

(1) (Existence) $\exists$ p_i's irreducible s.t. $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$

(2) (Uniqueness) If $a = q_1 \cdot q_2 \cdot \cdots \cdot q_m$ and q_i's irreducible, then $m = n$ and $\exists\, \sigma \in S_n$, $p_i \sim q_{\sigma(i)}$.

We often prove these properties separately. Let's recall how we prove the existence part for $\mathbb{Z}$.

. If a is irred., we are done. If not, $a = bc$ and $b, c \notin \mathbb{Z}^\times$.

And so $|b|, |c| < |a|$. Therefore by repeating this argument

Lecture 18: Noetherian

Thursday, November 29, 2018 1:00 PM

for b and c, ... in finitely many steps we get to the desired decomposition. In general it is not clear if this process ends in finitely many steps:

$a = a_1 a_1'$; $a_1 = a_2 a_2'$; $a_2 = a_3 a_3'$; ... then

$\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$. If $a_i, a_i' \notin D^\times$, then

$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$. We would like to avoid this case.

Def. A ring A is called Noetherian if any non-empty chain of ideals has a maximum.

Lemma. A is Noetherian if and only if it satisfies the ascending chain condition (a.c.c.) ; that means

$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ and $\mathfrak{a}_i \lhd A$ imply $\mathfrak{a}_{n_0} = \mathfrak{a}_{n_0+1} = \cdots$ for some $n_0 \in \mathbb{Z}^+$.

Pf. ($\Longleftrightarrow$) $\{\mathfrak{a}_i\}_{i=1}^{\infty}$ is a non-empty chain of ideals. So it has a maximum, say $\mathfrak{a}_{n_0}$. So for any $i \geq n_0$, $\mathfrak{a}_{n_0} \supseteq \mathfrak{a}_i$ and $\mathfrak{a}_{n_0} \subseteq \mathfrak{a}_i$; thus $\mathfrak{a}_{n_0} = \mathfrak{a}_i$ for $i \geq n_0$.

Lecture 18: Noetherian

Thursday, November 29, 2018 1:20 PM

($\Leftarrow$) Suppose C is a non-empty chain of ideals. And suppose to the contrary that C does not have a maximum. We recursively define a sequence $\{\mathfrak{a}_i\}_{i=1}^{\infty}$ of ideals.

$\cdot C \neq \emptyset \Rightarrow \exists\, \mathfrak{a}_1 \in C$

. Suppose we have already defined $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ s.t.

$$\mathfrak{a}_i \in C \text{ and } \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_n .$$

Since C does not have a maximum, $\exists\, \mathfrak{a}_{n+1} \in C$ s.t. $\mathfrak{a}_{n+1} \not\subseteq \mathfrak{a}_n$. As C is a chain, $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$. Therefore we get a strictly ascending chain of ideals $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$ which is a contradiction. ∎

We will show the <u>existence part</u> of factorization for any Noetherian integral domain; but first we want to have a more structural understanding of Noetherian rings.

<u>Prop.</u> A is Noeth. $\Leftrightarrow$ any ideal of A is finitely generated. (Next lecture).